2014-09

How program managers can use whistleblowing to reduce fraud within government organizations

Ernst, Brian A.; Kubik, Jeffery J.; Cruz, Angel F.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

JOINT APPLIED PROJECT

HOW PROGRAM MANAGERS CAN USE WHISTLEBLOWING TO REDUCE FRAUD WITHIN GOVERNMENT ORGANIZATIONS

By: **Brian A. Ernst,**
Jeffrey J. Kubik, and
Angel F. Cruz

September 2014

Advisors: **Brad Naegle**
Charles K. Pickar

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2014	**3. REPORT TYPE AND DATES COVERED** Joint Applied Project	
4. TITLE AND SUBTITLE HOW PROGRAM MANAGERS CAN USE WHISTLEBLOWING TO REDUCE FRAUD WITHIN GOVERNMENT ORGANIZATIONS		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Brian A. Ernst, Jeffery J. Kubik, Angel F. Cruz			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

The objective of this project is to recommend how U.S. program managers can use whistleblowing policies to combat fraud within the Department of Defense. Whistleblowers are an underused asset for revealing hidden, immoral, fraudulent, or inappropriate actions within an organization. Not only may whistleblowing identify undetected problems, it may save lives and vast sums of money.

This research project answers the following questions: 1) Why is whistleblowing important to a program-management office and its chain of command? 2) What makes someone want to, or not want to, "blow the whistle" within their organization? 3) How can U.S. defense organizations position themselves to fully utilize the potential power of whistleblowing?

The history of whistleblowing in the United States, its positive and negative impacts, and whistleblower decision-making are discussed and an open-systems organizational model is used to demonstrate why a formal whistleblowing process is beneficial. Finally, recommendations are provided as to how organizations can create or strengthen their whistleblowing polices.

14. SUBJECT TERMS Whistleblowing, Whistleblowers Protection Act (WPA) 1989, The Whistleblower Protection Enhancement Act (WPEA) of 2012, fraud, False Claims Act			**15. NUMBER OF PAGES** 101
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

HOW PROGRAM MANAGERS CAN USE WHISTLEBLOWING TO REDUCE FRAUD WITHIN GOVERNMENT ORGANIZATIONS

Brian A. Ernst, Civilian, Department of the Army
Jeffrey J. Kubik, Civilian, Department of the Army
Angel F. Cruz, Civilian, Department of the Army

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN PROGRAM MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2014

Authors: Brian A. Ernst

Jeffery J. Kubik

Angel F. Cruz

Approved by: Brad Naegle

Charles K. Pickar

William R. Gates, Dean
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

HOW PROGRAM MANAGERS CAN USE WHISTLEBLOWING TO REDUCE FRAUD WITHIN GOVERNMENT ORGANIZATIONS

ABSTRACT

The objective of this project is to recommend how U.S. program managers can use whistleblowing policies to combat fraud within the Department of Defense. Whistleblowers are an underused asset for revealing hidden, immoral, fraudulent, or inappropriate actions within an organization. Not only may whistleblowing identify undetected problems, it may save lives and vast sums of money.

This research project answers the following questions: 1) Why is whistleblowing important to a program-management office and its chain of command? 2) What makes someone want to, or not want to, "blow the whistle" within their organization? 3) How can U.S. defense organizations position themselves to fully utilize the potential power of whistleblowing?

The history of whistleblowing in the United States, its positive and negative impacts, and whistleblower decision-making are discussed and an open-systems organizational model is used to demonstrate why a formal whistleblowing process is beneficial. Finally, recommendations are provided as to how organizations can create or strengthen their whistleblowing polices.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACFE	Association of Certified Fraud Examiners
ATK	Alliant Techsystems Inc
CIA	Central Intelligence Agency
DDRE	Director, Defense Research and Engineering
DOD	Department of Defense
DODIG	Department of Defense Inspector General
ERC	Ethics Resource Center
FBI	Federal Bureau of Investigation
GAP	Government Accountability Project
IRS	Internal Revenue Service
MSPB	Merit Systems Protection Board
NCIS	Naval Criminal Investigative Service
OSHA	Occupational Safety and Health Administration
PWC	PricewaterhouseCoopers
PM	Program manager
SEC	Securities and Exchange Commission
SECIG	Securities and Exchange Commission Inspector General
USC	United States Code
WPA	Whistleblower Protection Act
WPEA	Whistleblower Protection Enhancement Act

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. UNDERSTANDING FRAUD

Fraud is a global plague to which no organization is immune. The world's largest anti-fraud organization, the Association of Certified Fraud Examiners (ACFE), estimates that a typical organization loses 5 percent of revenue each year to fraud (ACFE, 2014) (Ratley, 2014). When this percentage is applied to the 2013 estimated gross world product of $73.87 trillion, a projected fraud loss of nearly $3.7 trillion in 2014 (Ratley, 2014) is revealed.

Fraud cannot be entirely contained, and it continues to spread. The $3.7 trillion statistic above was estimated using data that was actually detected and reported. If every instance of fraud were reported, this estimate of loss would undoubtedly be much higher. The U.S. government is gravely concerned with fraud within its organizations. While acknowledging that fraud will never be eradicated, the U.S. seeks ways to improve fraud detection and thus reduce losses.

To detect and prevent fraud, it is important to understand who is committing the offense and why. Utilizing poll results forensic experts in the U.S. categorize the general population into three groups: 20 percent who would never commit fraud, 60 percent who would if the chance of getting caught were low, and 20 percent whom seek ways to commit fraud regardless of the circumstances (Brooks & Dunn, 2010). It is a sobering notation that up to 80 percent of the U.S. population would commit fraud if given the right opportunity. Fraud opportunities are a critical part of the fraud-triangle model.

The fraud-triangle model was developed from criminologist Donald R. Cressey's hypothesis that,

> Trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-sharable, are aware this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property. (Cressey, 1973)

According to the fraud triangle, depicted in Figure 1, three factors must be present for an ordinary person to commit fraud: pressure, opportunity, and rationalization.

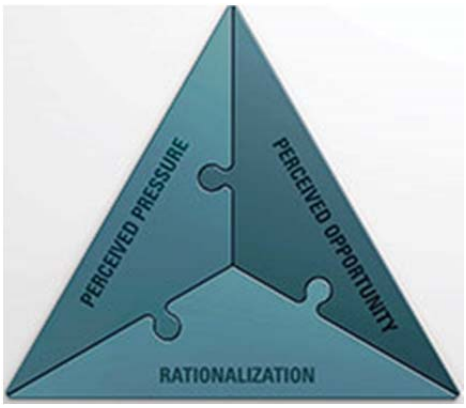

Figure 1. The Fraud Triangle (from Albrecht, 2014)

The first side of the fraud triangle is *pressure* as a motivating factor. An individual might have a financial problem, such as unanticipated medical bills, or a perceived financial need, for instance, wanting to purchase something but lacking the means to do so. The motivation might also be nonfinancial—for example, high pressure to meet performance goals at work or cover up a coworker's mistakes.

Once this pressure is perceived as unbearable, the soon-to-be perpetrator begins to rationalize the contemplated fraud. *Rationalization* is the second side of the triangle. The individual may see himself as an ordinary, honest person who is merely among the 60 percent who are caught in a bad set of circumstances. The potential fraudster finds it necessary to mentally justify the crime as an acceptable or defensible act.

The final side of the triangle is the *opportunity* to commit fraud—access to assets and information that the employee can use both to commit and conceal the fraud. Opportunity can be created by weak internal controls or poor managerial oversight. The fraud-bent individual must see a way to use his position of trust to alleviate personal pressure and assess a low risk of being discovered. Almost three quarters (73 percent) of respondents to the 2014 PwC Global Economic Crime Survey indicated that the

opportunity or ability to commit a crime was the most important factor in the crime's execution by an internally placed fraudster (Skalak, 2014).

An organization has significantly more control over the opportunity side of the fraud triangle than over pressure and rationalization. The organization can mitigate the risk of fraud by reducing opportunities by means of internal policies, processes, and controls. A key resource that program managers can promote is whistleblowers (Cressey, 1973).

B. WHISTLEBLOWING

According to the *Merriam-Webster Dictionary,* a whistleblower is one "who reveals something covert or who informs against another." The U.S. Office of Special Counsel (U.S. Office of Special Counsel, 2014) describes five types of fraud or wrongdoing:

1. Violation of a law, rule, or regulation
2. Gross mismanagement
3. Gross waste of funds
4. Abuse of authority
5. Substantial and specific danger to public health or safety

A whistleblower is generally an employee of a private or public institution who is on the lookout for individuals (especially those in supervision or authority) who are doing wrong. Often a whistleblower simply happens to be in the right place at the right time to witness a wrongdoing perpetrated upon a company, institution, or the public good. The list of prominent American whistleblowers includes the following:

- Daniel Ellsberg, who leaked a top-secret Pentagon study of U.S. government decision-making in relation to the Vietnam War to the Senate Foreign Relations Committee, the *New York Times*, the *Washington Post*, and 17 other newspapers. Ellsberg was tried under the Espionage Act (Lemann, 2002).
- Gregory Hicks, a state-department employee and former deputy chief of mission in Libya who testified before Congress about attacks on an

American diplomatic facility in Benghazi. Hicks was subsequently demoted from his position (Zornick, 2013).

- Sherron Watkins, an Enron Corporation vice-president who exposed one of the largest accounting frauds in history. Watkins feared for her safety while being bounced from job to job within Enron and endured threats of dismissal (Pasha, 2006).
- Kendall Dye, an Alliant Techsystems program manager who uncovered testing shortfalls in a military flare program and jeopardized a 21-year career by preventing his company from knowingly delivering unsafe products to the U.S. government (Glater, 2008)

This research focuses on what program managers and other leaders within an organization can do to strengthen whistleblowing policies. Whistleblowing happens when an individual reports or discovers evidence of a wrongdoing. The critical questions for those seeking to encourage reporting of the offense are as follows:

- What motivates an individual to blow the whistle?
- What are their incentives, disincentives, and ethical and moral dilemmas when deciding to report?
- Is the organizational culture promoted by the program manager conducive to whistleblowing?
- Will others in the organization react favorably or unfavorably to the whistleblower?

Too often, U.S. defense organizations view whistleblowers in a defensive and negative light. This research project explores what organizations can do to reverse this perception and make whistleblowing work for them through sound policy. In developing a whistleblower policy, program managers must look at organizational structures, culture, processes, and above all, human nature. A policy that facilitates whistleblowing can help employees and organizations better align their responses to wrongdoing, to yield a better place to work and build a stronger institution overall. Finally, this research provides recommendations on how to design and implement whistleblowing policies within an organization.

C. PURPOSE OF RESEARCH

Two major phenomena were explored in the conduct of this research: first, the act of whistleblowing itself. What leads an individual to blow the whistle? Does the

whistleblower generally realize the full implications of his actions? Did his whistleblowing have any impact on himself or the organization? Second, from a program manager's perspective, what framework can be devised to utilize the information provided by whistleblowers? The PM's organization must have proper structures, processes, and cultural factors in place to allow the development of policy and create a context for whistleblowing. Employees and management within the program-management office must share a common view of wrongdoing, agree on what constitutes blowing the whistle, and ensure appropriate reporting mechanisms are in place. When employees and management agree, program managers are in a better position to reduce waste and corruption, employee input is affirmed, and the entire organization can expect to grow stronger and more effective overall.

D. RESEARCH QUESTIONS

This study addresses the following questions:

1. Why is whistleblowing important to a program-management office and its chain of command?
2. What makes a person want to—or decline to—blow the whistle within his organization?
3. How can U.S. defense organizations develop policies to capitalize on the potential benefits of whistleblowing?

Answers to these questions were sought by reviewing a large literature on fraud and whistleblowing, consisting of case studies, articles, websites, and books. From the many broad topics discussed, recommendations were distilled as to how organizations can use whistleblowers to improve their fraud controls. Chapter II of this report explores the development of whistleblowing policies and reforms. Chapter III focuses on fraud detection through whistleblowing. The whistleblowing decision-making process is presented in Chapter IV, including incentives and disincentives to employees and other personnel. Chapter V uses an open-system organizational model to analyze the impacts of an established whistleblowing policy, or lack thereof, and Chapter VI makes recommendations on how an effective whistleblowing policy may be implemented, including strategy and execution.

THIS PAGE INTENTIONALLY LEFT BLANK

II. DEVELOPMENT OF WHISTLEBLOWING POLICIES AND REFORMS

Whenever individuals in places of power and decision see ways to achieve greater power, influence, or prosperity by their actions, it is human nature that some persons will be tempted to exploit the situation. It is also human nature that whistleblowers sometimes arise to report an illegal or unethical act perpetrated upon a company, stockholders, or, in the case of governmental abuse, the people. When whistleblowers act, those who have committed the illegal or unethical deed often seek to retaliate, and may have resources to do so.

A. THE FIRST KNOWN WHISTLEBLOWERS IN AMERICAN HISTORY

In 1777, just outside of Providence, Rhode Island, ten sailors, under the direct command of the commander in chief of the Continental Navy, Commodore Esek Hopkins (Kohn, 2011) sent a petition to the U.S. Congress alleging misconduct by Commodore Hopkins. The men stated that their commander could no longer lead them due to questionable decisions, including failing to attack a British frigate that had run aground, permitting the enemy to escape, and treating prisoners in a cruel and inhumane manner (Kohn, 2011). The Continental Congress and its president, John Hancock, investigated the accusations, found them true, and suspended Commodore Hopkins, eventually relieving him of his duties. At the time, Hopkins was America's highest-ranking naval officer and the U.S. was waging a war.

The exposure of this decommissioned officer came at a price. Commodore Hopkins publically humiliated two of the sailors by parading them before a mock trial and relieving the "ringleader" of his duties. Thus, the first recorded whistleblower in U.S. history suffered retaliation (Kohn, 2011).

Fearing further reprisals, the sailors asked Congress for protection. They received free legal representation, along with payments for court costs and attorney fees. The first Congress "understood that finding whistleblowers guilty of criminal libel was counter to the framework of the new Republic" (Kohn, 2011, p. 199); however, no whistleblower

protection law was enacted at that time. Before the term was coined or any laws on the topic were drafted, these sailors showed the important role whistleblowers would have in the newly formed country.

B. THE FALSE-CLAIMS ACT

The False-Claims Act (FCA), or Lincoln Law, of 1863 was the predecessor to the modern basis of whistleblower law, the Whistleblower Protection Act (WPA) of 1989. Learning of unscrupulous defense contractors who were trying to profit unfairly during the Civil War, President Abraham Lincoln won the right for citizens to serve as government enforcers through false-claims lawsuits (Devine, 2011). The purpose of the act was to discover anti-government fraud and encourage cognizant citizens to provide information. (History of the False-Claims Act, 2013). Whistleblower provisions allowed private parties to sue companies and individuals on behalf of the government and allowed them to collect up to 50 percent of monies recovered. The FCA remained virtually unchanged until 1943, when, responding to pressure from large defense contractors during WWII, lawmakers cut the potential award size, thus removing a powerful incentive to inform.

C. THE WHISTLEBLOWER PROTECTION ACT (1989)

Many post-war events led to the strengthening of whistleblower-protection laws. Perhaps the most influential were the Watergate scandal in the 1970s and increased military fraud, waste, and abuse in the 1980s, during the Cold War. President Ronald Reagan formed the Packard Commission to investigate defense-contractor fraud, with its tales of $400 hammers and $600 toilet seats (Kurland, 1993). In 1985, a Department of Defense report stated that 45 of the largest hundred defense contractors, including nine of the top ten, were under investigation for multiple fraud offenses (Defense Procurement Fraud, 1985). Because employees hesitated to speak up due to fear of reprisals, it was difficult for the Justice Department to bring perpetrators to account. Employees were reasonably afraid of losing their jobs for reporting fraud and abuse. To clean up the defense landscape, two senators, Charles Grassley (R–IA) and Howard Berman (D–CA), sponsored a 1986 amendment that strengthened the False-Claims Act (Devine, 2011) by

providing greater monetary incentives for whistleblowers to come forward and creating monetary and other incentives for private attorneys to independently investigate fraud. Before this amendment, civil-fraud recoveries averaged between $6M–$9M per year. Starting in 1986 and for the next 21 years, recoveries totaled nearly $24 billion—a staggering increase. In 2009 alone, false-claims lawsuits led to $5.6 billion in recoveries (Devine, 2011). Most importantly, the adversarial perception of whistleblowers was turning, and government organizations and corporations began to spend substantial sums on meaningful compliance programs (Devine, 2011).

Despite this amendment, whistleblowers remained vulnerable to retaliation. By reporting illegal or unethical behavior, a whistleblower could be demoted, fired, or, in extreme cases, imprisoned. Following the strengthening of the FCA, the U.S. Congress passed the Whistleblower Protection Act (WPA) of 1989 for federal employees who made disclosures of illegal or improper government activities. The protections of the WPA covered most executive-branch employees if a negative personnel action was made against them due to a disclosure (Whitaker, 2007). A federal agency is in violation of the WPA if authorities take or threaten retaliatory personnel action against any employee because of information disclosed. Under the WPA, whistleblowers may file complaints alleging violation of a law, rule or regulation; gross mismanagement; gross waste of funds; abuse of authority; or substantial and specific danger to public health or safety.

D. THE WHISTLEBLOWER PROTECTION-ENHANCEMENT ACT (2012)

After the WPA was enacted in 1989, legislators continued to look for ways to improve the law and increase its scope. Congress made several attempts before passing the Whistleblower Protection-Enhancement Act (WPEA) in 2012. Its three broad provisions are as follows:

- Expanded protection for disclosures of government wrongdoing
- Expanded coverage and fair processes
- Enhanced education and understanding concerning whistleblower rights

The new law closed judicially created loopholes that had removed protections for the most common whistleblowing scenarios and left only token rights. The law also

expanded coverage of employees to include those from the Transportation Security Administration (Whistleblower Protection Enhancement Act of 2012, 2012) and protected government scientists who challenged censorship (Whistleblower Protection Enhancement Act of 2012, 2012). The WPEA overturned the Merit Systems Protection Board (MSPB) practice that allowed agencies to present a defense first in some cases and allowed the MSPB to make a ruling before hearing evidence of retaliation (Whistleblower Protection Enhancement Act of 2012, 2012). This was significant in that whistleblowers had to present any claim of retaliation before the MSPB and prove that their actions had resulted in derogatory personnel actions. If a whistleblower lost his case before the MSPB, his recourse was an appeal before the Federal Circuit Court of Appeals, which had sole jurisdiction on review. The WPEA suspended this procedure (Whistleblower Protection Enhancement Act of 2012, 2012) under which, according to Devine, Devine, and Blaylock, the court ruled against whistleblowers 226 of 229 times (a rate of 98.7 percent) from October 1994–May 2012 (2012).

E. OTHER WHISTLEBLOWER REFORMS

The Corporate and Criminal Fraud Accountability Act of 2002, also known as the Sarbanes–Oxley Act, provided sweeping reforms in the way that public disclosures are made and accounted for by publicly held corporations under federal securities laws (Watnick, 2007). Bumgardner (2003) noted that Congress rushed to pass this complicated law in the wake of the Enron and WorldCom corporate scandals. Section 401 of the legislation encourages employees, directors, and supervisors in the corporate world to look for and report fraud within their companies. Along with this encouragement came other significant protections. A problem with the Sarbanes–Oxley Act, however, is that whistleblower cases, which are meant to be adjudicated quickly, are often stalled far beyond the maximal period mandated (Watnick, 2007).

Sarbanes–Oxley allows for an employee who has been retaliated against to be reinstated in his previous position if he can show by a preponderance of the evidence that 1) he engaged in protected activity under Sarbanes–Oxley, 2) that his employer was aware of this activity, 3) that he suffered an adverse employment action, and 4) that the

protected activity was likely a contributing factor in the employer's decision to take adverse action (Watnick, 2007). The Sarbanes–Oxley Act did not go far enough, however, since whistleblowers found it difficult to obtain protection and relief (King, 2011). This played out during the financial crisis of 2007–2009, with the housing bubble, sub-prime mortgages, outsized risks, and overleveraging occurring commonly (King, 2011). During testimony in the felony fraud trial of Bernard Madoff, the Senate Banking Committee heard financial analysts advocate stronger whistleblower protections than those afforded under Sarbanes–Oxley. This led to the enactment of the Dodd–Frank Wall Street Reform and Consumer Protection Act of 2010 (King, 2011).

The purpose of Dodd–Frank was to restore public confidence in the financial system, prevent another crisis, and allow any future asset bubble to be detected and deflated before financial crisis ensued (Sweet, 2010). Dodd–Frank included a whistleblower program that allowed individuals reporting original information to the SEC that led to a recovery exceeding $1 million to obtain 10–30 percent of the recovery. The law also included a prohibition on retaliation (Dutta, 2012), by which a targeted individual has the right to reinstatement in his same position, twice the amount of back pay plus interest, and compensation for litigation costs, expert-witness fees, and reasonable attorney fees (15 USC § 78u–6 (h)(1)(C)). Given these penalties, it behooves organizations and corporations to install effective fraud-reporting policies so that internal problems can be resolved without federal-government involvement.

To achieve effective fraud-reporting policies, organizations need to cultivate and communicate a culture in which the reporting of fraud is considered welcome and necessary. Leadership must understand the value of whistleblowing as not only curtailing a specific incidence of fraud, but as beneficially exposing the internal weaknesses that allow fraud to occur. Thus the government encourages all employees to blow the whistle, incentivizing them by offering monetary rewards for their service.

THIS PAGE INTENTIONALLY LEFT BLANK

III. FRAUD DETECTION THROUGH WHISTLEBLOWING

Well established, implemented, and controlled whistleblowing policies should be a key part of an organization's internal checks and balances. Human beings are far from perfect in their behaviors. As the "I'm only human" excuse implies, some wrongdoing is unintentional—simple human mistakes that happen despite innocent motivations. In contrast is the deliberate misconduct of persons who intentionally break rules or laws for personal or corporate gain. This chapter examines historical and other data to suggest the necessity of implementing internal processes to reduce damage and loss from fraud.

In the DoD, program managers (PMs) are required to operate under very specific rules. The Federal Acquisition Regulation (FAR) provides PMs with DoD-mandated policies and procedures for legally completing acquisitions. The DoD Inspector General enforces Instruction Number 7600.02, which lays out audit directions and policies that must be met to comply with DoD requirements. (IG DOD, 2007). Several Army regulations govern acquisition programs, chief of which is Army Regulation 70-1, the Army Acquisition Policy. This regulation is used to manage acquisition programs following statutory requirements, the FAR, the Defense Federal Acquisition Regulations supplement, other DoD regulatory direction, and other Army federal-acquisition-regulation supplements (Headquarters, Department of the Army, 2011).

The FAR provides almost no guidance on fraud prevention and whistleblowing, stating only that contractors and subcontractors must observe regulations against discharging, demoting, or otherwise discriminating against an employee in reprisal for whistleblowing. The FAR also requires contractors to display fraud-hotline posters.

The Inspector General (IG) instruction to PMs on audit policies provides thorough guidance on the who, what, why, and where of audit requirements. Internal and external audits in 2013 accounted for 17.1 percent of the fraud examined by the Association of Certified Fraud Examiners (Ratley, 2014). However, echoing the FAR, IG documents provide no guidance on how to leverage a highly effective and low-cost resource to combat fraud—namely, whistleblowers.

A. EFFECTIVE LEVERAGING OF *QUI TAM* PROVISIONS

The provision in the FCA by which citizens may serve as government enforcers is known as *qui tam*, an abbreviation of the Latin for "he who sues in this matter for the king as well as for himself." *Qui tam* is a unique legal mechanism that allows citizens with evidence of fraud against government contractors and programs to sue to return the stolen funds to the government (False, 2014). The government shares a portion of the recovered money with the party who filed charges.

Under the FCA, in fiscal year 2013, the Department of Justice recovered $3.8 billion in direct fraud against the government (Brainin, 2013). Of that total, $2.9 billion was recovered directly due to whistleblowers (USDOJ, 2014). Although the total money recovered in 2013 was less than in the previous fiscal year, it was the second-highest total recovered in a single year. And while 2013 did not break the overall financial-recovery record, it did break the record for number of cases filed and for the amount of money recovered specifically under procurement-fraud suits ($887M). In 2013, whistleblowers also played a large role in the filing of FCA lawsuits, with 753 of 846 new cases initiated under *qui tam* provisions (Fraud, 2013).

As shown in Figure 2, starting in FY1995, *qui tam* suits became the primary source of recovery information under the FCA. Figure 2 also shows that the FCA processes an increasing number of lawsuits each year, increasingly initiated by whistleblowers under the *qui tam* provision.

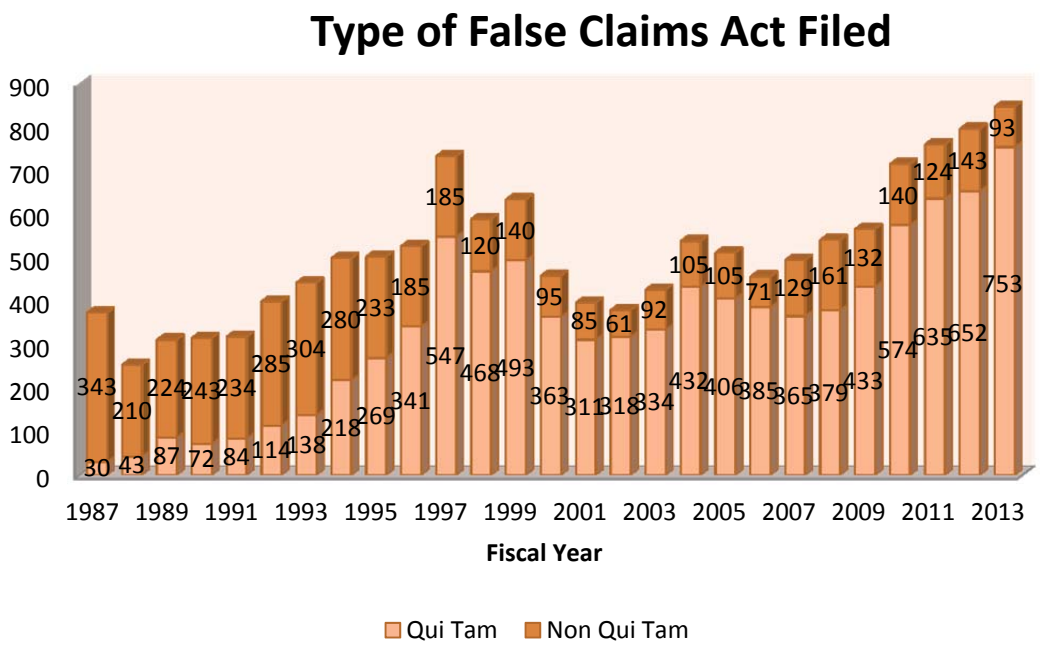

Figure 2. Types of False-Claims Act Files (after Fraud, 2013)

The overall historical success of the FCA is largely due to the 9,244 *qui tam* lawsuits that whistleblowers have filed since FY1987, when the FCA was amended. Overall, since 1987, whistleblower *qui tam* cases have led to more than $27.2 billion in government recoveries, with half of that amount ($13.5 billion) recovered in the past five years (Fraud, 2013).

The fact that the FCA continues to set new records for money recovered and number of *qui tam* filings suggests that fraud against the government remains an active threat that needs to be deterred, exposed, and eliminated.

B. INDEPENDENT SURVEY RESULTS

The 2014 Global Economic Crime Survey conducted by PricewaterhouseCoopers (PWC), the world's largest professional-services firm, included data from over 5,000 respondents in 95 countries. This survey confirmed the data presented earlier in relation to the FCA—massive economic crime is a fundamental fact of life for every segment of the global business community.

PWC determined that fraud constitutes one of the biggest problems of organizations worldwide and that organizations cannot rely solely on fraud controls such as internal audits to deter, detect, and defeat fraud. Figure 3 provides PWC survey data indicating that fraud occurs within government more than within most of the private industrial base (Parton, 2009, 2011; Skalak, 2014).

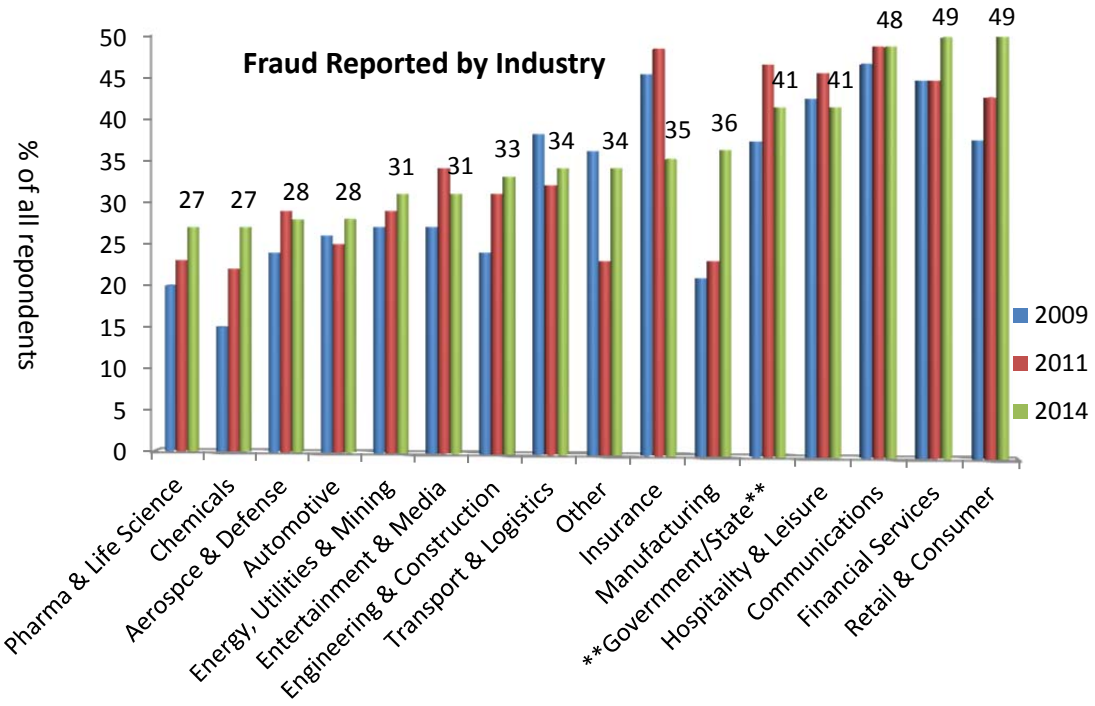

Figure 3. Fraud Reported by the Type of Industry
(after Parton, 2009, 2011; Skalak, 2014)

The Ethics Resource Center (ERC) also provides data comparing fraud within government and industry. The ERC is a nonprofit, nonpartisan organization dedicated to independent research that advances ethical standards and practices in public and private institutions (Ethics, 2014). The ERC polled government employees to determine what percentage had observed fraud in the reporting year. As shown in Figure 4, the government employees witnessed the same or greater instances of fraud as compared to employees of private businesses (Harned, 2007).

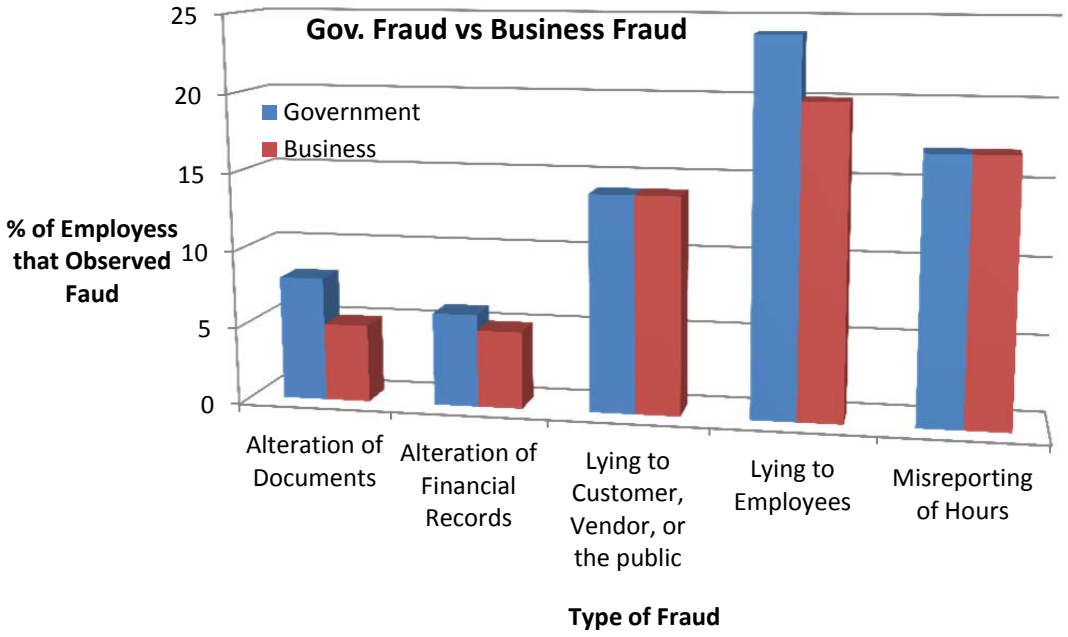

Figure 4. Fraud Witnessed within the Government and Private Business (after Harned, 2007)

The ACFE's 2014 *Report to the Nations on Occupational Fraud and Abuse* reveals over 1,400 cases of occupational fraud, as reported by investigating certified fraud examiners. In the ACFE report, tips proved the most common method of exposing occupational fraud. Figure 5 shows tips as most effective method of fraud detection for the past three reporting years (Ratley, 2014).

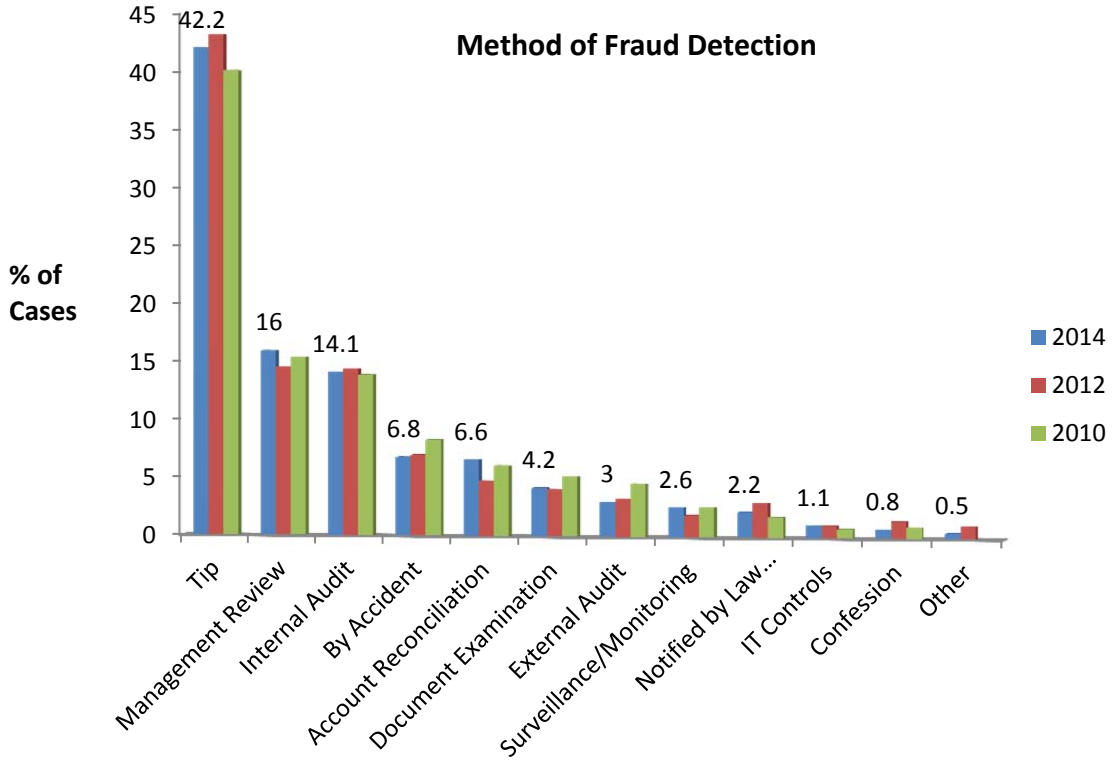

Figure 5. Methods of Fraud Detection (after Ratley, 2014)

Certified fraud examiners recognize that fraud, by its very nature, resists scientific observation and precise measurement. Fraudsters typically keep their actions secret from everyone not involved in the scheme; thus analysis is limited to fraud that has been detected and reported. For this reason having proactive whistleblowers who often work alongside the fraudster are essential to an effective anti-fraud program. As shown in Figure 6, the ACFE's report found that 49 percent of fraud cases analyzed was reported by employees, a statistic significantly higher than the PricewaterhouseCoopers finding of 23 percent (ACFE, 2014; Skalak, 2014). What both these data points show is that employees can provide a significant benefit to an organization's fraud-control system. Thus employees should be encouraged to report illegal or suspicious behavior and reassured that reports can be confidential and retaliation is prohibited.

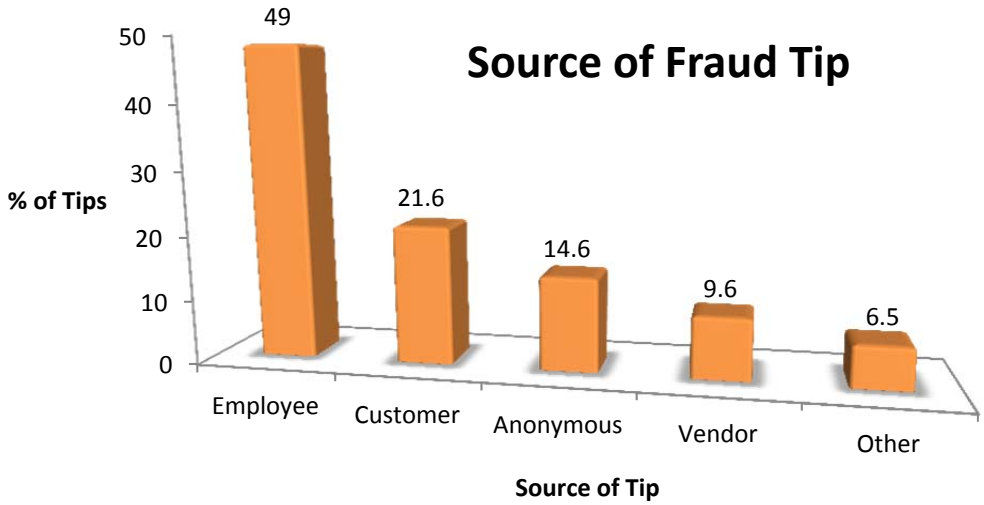

Figure 6. Source of Fraud Tips (after ACFE, 2014)

In 2007, the Ethics Resource Center conducted a survey of 3,452 U.S. employees, 774 of whom were federal employees (Hamed, 2007). The responses from federal employees were published as the *National Government Ethics Survey*. While the ERC subsequently published reports on private business ethics, no update on federal employees has been released.

The ERC's government survey mirrored those of PricewaterhouseCoopers and the Association of Certified Fraud Examiners in concluding that organizations need effective whistleblowing policies to minimize fraud. The ERC survey focused on ethics and misconduct, anticipating a rise in misconduct if deliberate action is not taken.

The ERC study found that one in four government employees works in an environment conducive to misconduct (Hamed, 2007). Several problems are inherent in such environments, two of which relate directly to the fraud triangle: employees encounter opportunities to do wrong and typically feel pressure to commit dubious acts. Figure 7 shows that pressure to compromise standards in order to complete required work tasks has been on the rise for government employees since 2003 (Hamed, 2007).

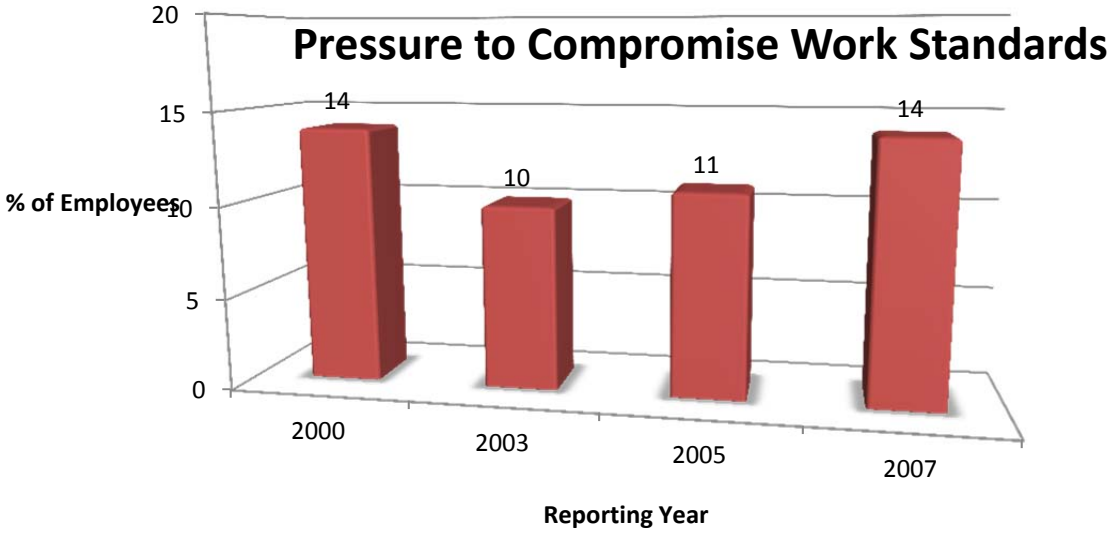

Figure 7. Pressure to Compromise Work Standards (after Harned, 2007)

Over half (52 percent) of federal employees polled by the ERC observed misconduct in their workplace, of which 25 percent chose not to report it (Harned, 2007). An employee failing to report misconduct creates a ripple effect that leaves management unaware of the problem, making it difficult to prevent further occurrences.

The PricewaterhouseCoopers, Association of Certified Fraud Examiners, and Ethics Resource Center studies confirm via global data spanning multiple years that whistleblowers can objectively help their organizations and that strong policies are needed to encourage whistleblowers to act. Whistleblowers may not only save the government millions of dollars, but the lives of innocent persons as well, as illustrated in the Alliant Techsystems case.

C. ALLIANT TECHSYSTEMS INC (ATK) CASE STUDY

Kendall Dye placed his career in direct jeopardy for the welfare of others when he blew the whistle on his employer, ATK Launch Systems. ATK ultimately paid $36.9 million in cash and services to settle his suit (Foy, 2014) alleging reckless disregard and deliberate ignorance of critical safety defects in munitions.

In 2005, Mr. Dye became the flare-program manager at ATK. Unlike the small flares used by commuters stranded on a highway, an ATK flare is a three-foot aluminum tube filled with thirty-six pounds of propellant that burns at more than 3,600°F (note that common steel melts at 2,500°F and aircraft aluminum melts at 1,250°F [Gagnon, 2011]) (Riley, 2012). Once ignited, a flare cannot be extinguished and must burn itself out. One method to deploy the flares is to release them from airplanes, attached to parachutes. The flares illuminate approximately a square mile of the ground below for several minutes. If one of these flares were to accidently ignite, it could easily set fire to its surroundings, setting off nearby ordnance, burning a hole in the steel hull of a ship, or melting through the aluminum skin of an airplane.

The same year Mr. Dye became the flare-program manager, the Navy evaluated whether the flares could meet a more stringent four-foot-drop requirement versus the then-current requirement of surviving a ten-foot drop without igniting. The Navy found that the flares ignited at drop heights of forty, thirty, and twenty feet, but did not test them at ten feet. Mr. Dye initially thought the plastic igniter, which was designed to break when deployed, could be made more rugged to meet naval requirements. During his redesign of the plastic igniter, Mr. Dye discovered that the plastic igniter could break and cause ignition from a fall of just 11.5 inches.

After sifting through old ATK records of the flare program, Mr. Dye learned that in the late 1990s, military buyers complained of the flares failing to ignite after deployment. ATK had a team of engineering students from a local university design an "improved" igniter. The student team came up with a system that used the force generated by the flare's parachute opening to snap a thin piece of plastic, which activated the flare's ignition. Mr. Dye found an email from the ATK test engineer assigned to evaluate the design that warned about a "more realistic scenario, which might present a significant hazard to equipment/personnel: If the flare assembly receives a significant impact (i.e., dropped) I can foresee" the plastic restraint in the igniter breaking, "resulting in complete ignition of the flare." In his email, the test engineer recommended performing drop tests to gauge the safety of the flares with the new igniter design. ATK

started shipping the redesigned flares fitted with the plastic igniter, without testing, in 2000 (Glater, 2008).

Upon finding the test-engineer's email, Mr. Dye notified his supervisor, who told him not to tell anybody—the issue would be handled internally. ATK formed a team to review the flare program and design, but blamed a third-party vendor for modifying the flares and did not focus on the student-redesigned element. ATK also sent a letter to its customers stating the flares may be more sensitive than specifications allowed if dropped.

Mr. Dye did not see ATK take any steps to actually correct the issue, including fixing or replacing the flares that had already been delivered to the U.S. government, so he decided to blow the whistle through the FCA. In April 2012, ATK was ordered to pay $21 million to the government to settle Mr. Dye's *qui tam* suit. ATK was also required to retrofit the 76,000 defective flares in government inventory.

Fortunately, Kendall Dye was willing to jeopardize his 21-year career and expose the company's knowing delivery of hazardous products before any accidents occurred (Glater, 2008).

IV. THE WHISTLEBLOWING DECISION-MAKING PROCESS

The whistleblower decision-making process is that by which an individual determines whether to report a wrongdoing in an organization. There are many factors in this decision, centering on incentives. This chapter explores the perceived incentives and disincentives of whistleblowing.

A. INCENTIVES

Deciding to blow the whistle begins with moral values and the individual's ability to negotiate the difference between right and wrong. Once a potential whistleblower takes a moral position, other incentives come into play. This section explores how the type of wrongdoing affects the decision-making process and rationale, discusses whether some types of wrongdoing are more likely to be reported, and evaluates several monetary-reward systems and legal protections currently in place.

1. Moral Values

Moral values play a large role in whistleblowing. Morality can be defined as a system of duties or rules between people with which both parties are required to comply (Robertson, 2010). Notice that this definition does not define what differentiates right from wrong. It essentially defines morality as a set of mandatory rules within a social structure.

Interpretation as to what is right or wrong is subject to the development of moral values that are realized through an individual's life experiences. Such realizations take place through socially established rules, policies, and procedures. It is assumed that moral values are not self-constructed, but rather correspond to a societal paradigm that is accepted and helps define judgments (Avakain & Roberts, 2011).

Thus the morality of a whistleblower is defined in accordance with social and corporate rules, moral norms, and principles (Coady & Bloch, 1996). Conversely, an example of immoral organizational behavior is offering or accepting a bribe. If a government organization were to award a contract as a result of bribery, not only would

the corporate rules (laws) be broken, but the common principle of fairness as well. In this example, a potential whistleblower would likely have a moral problem with wrongdoing, but simply acknowledging that an action is immoral is not sufficient motivation for an individual to report the activities. Rather, it is only the first step in the decision-making process.

Whistleblowers often display concern when a breach of moral values harms the welfare of others (Avakain & Roberts, 2011); indeed, concern for others is a common theme in nearly all the whistleblowing cases encountered in this research. It is inferred that seeking the wider social good beyond personal wellbeing plays into the typical whistleblower decision-making process and provides as an incentive to follow through. The ATK case study expresses this point. Upon becoming the flare-program manager, Mr. Dye learned that previously fielded flares were potentially hazardous to personnel and equipment. He felt that his company's indifference to these findings was immoral, and, motivated by concern for users, blew the whistle. Even though the informer was not directly impacted by the wrongful act, concern for others provided a strong motivation.

It is important to stress that the data does not suggest that "the welfare of others" is always a primary motivating factor—benefit to others may be no more than a byproduct. All organizations have stakeholders and parties with vested interests, and blowing the whistle on any illegitimate or immoral act will benefit some others in some way. In government organizations, the stakeholder is often identified as the taxpayer. If government waste is exposed in a whistleblower case, the taxpayer will benefit, but may not have been a factor in the whistleblower's decision.

A key aspect of the decision is an individual's perception of duty and its importance in his moral system (Avakain & Roberts, 2011). Duty is a feeling of responsibility to uphold what is morally just in a person's eyes—"The decision to act is driven by a personal concern that is based on values that uphold moral principles" (Avakain & Roberts, 2011, p. 77). Avakain and Roberts explain that a whistleblower's social concern does not develop at random, but is intertwined with a personal morality, which generates a sense of perceived duty. An example is Cynthia Cooper, whom *Time Magazine* named among its "persons of the year" for 2002. Unearthing a $3.8 billion

accounting fraud at WorldCom, Cooper stated, "We don't feel like we are heroes. I feel like I did my job" (Near et al., 2004, p. 219). This sentiment correlates with the sense of duty cited by Avakain and Roberts—Cooper felt it was her duty and responsibility to pursue what was morally right.

The association between a given wrongful corporate act and the whistleblower's morality is of the utmost importance in determining how the whistleblower interprets the act vis-à-vis the wider social good (Avakain & Roberts, 2011). It is understood that morality plays a paramount role in decision-making, but are some types of wrongdoing more likely to be reported than others?

2. Type of Wrongdoing Effects on the Whistleblowing Decision-Making Process

Data was analyzed from a survey of employees of a large military base to assess possible differences in the whistleblowing decision based on the types of wrongdoing observed (Near et al., 2004). The findings, published in *Business Ethics Quarterly* in 2004, analyzed types of wrongdoings and correlated reasons for not reporting, costs associated with the wrongdoing, quality of evidence, and anticipated retaliation.

The survey looked at approximately 10,000 employees at a base in the United States. Roughly two-thirds were civilian; the other third were active military personnel. The base acquires high-tech aircraft and support systems, medical care, and base support, with budgets that run into the billions of dollars. The survey was sent to 9,900 employees, with a cover letter from the base commander requesting it be filled out anonymously. A total of 3,288 employees completed and returned surveys to the researchers (about 33 percent).

Employees were asked if they had "personally observed or had direct evidence" of any wrongdoing identified in the survey within their organization in the last twelve months. Thirty-seven percent (1,224 employees) responded affirmatively. All other employees (those with negative responses) were excluded from further analysis. Those who observed wrongdoing were asked additional questions regarding the activities they

considered most serious or which had greatest impact on themselves personally (Near et al., 2004).

The researchers grouped the wrongdoings identified into seven categories (Near et al., 2004) as defined below.

- *Stealing* (10 percent of identified wrongdoings): Theft of federal funds, stealing of federal property, accepting bribes or kickbacks, use of official position for personal benefit, unfair advantage to a contractor, and employee abuse of office
- *Waste* (44 percent): Waste by ineligible persons receiving benefits, by a badly managed program, or of organizational assets
- *Mismanagement* (11 percent): Management cover-up of poor performance and false projections of performance
- *Safety Problems* (8 percent): Management's permitting unsafe or non-compliant products and unsafe working conditions
- *Sexual Harassment* (8 percent): Unwelcome sexual advances or requests for sexual favors and verbal or physical contact of a sexual nature
- *Discrimination* (13 percent): Any discrimination based on race, sex, religion, etc.
- *Violation of Law* (7 percent): Any legal violation

The researchers asked those who observed offenses whether the incident was reported to an immediate supervisor, higher-level supervisor, higher-level agency official, agency inspector general, or any of several external channels. Of those who observed wrongdoing, 74 percent made no report. The remainder was asked if they had been identified as the source of a written, reported case. Of those who blew the whistle, 77 percent were identified as the source, versus 23 percent who were kept anonymous.

The researchers contacted those respondents who had not reported an observed wrongdoing and asked them to complete a checklist of several reasons they did not report. The possible answers were, it was not part of my job; I didn't want to get coworker/supervisor in trouble; it was not serious enough; I wasn't sure who to report to; it was already reported; nothing could be done; reporting was too risky; and nothing would be done (Near et al., 2004).

To probe whistleblower retaliation, the researchers targeted those 77 percent of the whistleblowers who were identified as the source of a report to see how many experienced retaliation. Thirty-seven percent reported some type of retaliation, as detailed later in this chapter (Near et al., 2004).

Finally, the respondents were asked to describe the sequence of events surrounding the wrongdoing in question. Questions were made as the estimated costs associated with the wrongdoing, the frequency of occurrence, and the quality of evidence obtained in support of allegations. The cost question was framed as a range, since a specific dollar amount might be difficult to reasonably estimate. Thus, to the query, "if a dollar value can be placed on the activity, what was the amount involved," the available responses were "less than $999" (coded "$500"), "$1,000-$100,000" (coded "$55,000"), or "more than $100,000" (coded "$100,000"). The mean of the costs coded was $34,759, with a standard deviation of $49,755.

In some instances, such as sexual harassment, a dollar amount was not associated with the wrongdoing. The researchers therefore posed a second question, asking them to rate frequency of occurrence, as "once or rarely" (1), "occasionally" (2), or "frequently" (3). The mean score for frequency was 2.37, with a standard deviation of 0.93.

The last rating requested concerned the quality of evidence in support of the wrongdoing claim. The options available were written, physical, observed by witnesses besides the respondent, convincing to the respondent, convincing to a majority of other observers, and convincing to others who had nothing to gain or lose from the wrongdoing.

The researchers used chi-squared analysis to determine if differences in whistleblowing were significantly associated with a wrongdoing type. A chi-squared distribution is the sum of the squares of a set of normally distributed random variables. It is assumed the research team chose this method of analysis because the sum of random variables from any distribution can be closely approximated by a normal distribution, as the sum includes a greater and greater number of samples. Next, the team conducted an

analysis to assess whether wrongdoing type was significantly related to the conditions of the wrongdoing or to retaliation.

a. Analysis of Whistleblowing Compared to Wrongdoing Type

The data (Table 1) suggests that the type of wrongdoing committed was closely linked with whether witnesses actually blew the whistle. Legal violations were the most likely wrongdoing type to be reported—53 percent of those who observed legal violations reported the incident. Interestingly, legal violations were also the least observed of all wrongdoing types. Two other whistleblowing types stand out as being more likely to be reported: mismanagement (42.5 percent) and sexual harassment (40 percent).

Exploring the other end of the spectrum, waste and unfair discrimination were the least reported wrongdoings observed. For both, only about 17 percent of all observers blew the whistle. Waste and discrimination ranked as the highest-observed wrongdoing types in this study. In sum, the two most-observed wrongdoings on the military base were the two least-likely types to be reported.

Table 1. Chi-Square Analysis of Incidence of Whistleblowing, by Type of Wrongdoing (from Near et al., 2004)

	Inactive Observers	Whistle-blowers	Total Observers
Type of Wrongdoing			
Stealing			
Count	88	29	117
% within Type of Wrongdoing	75.2	24.8	100.0
% within Type of Observer	9.7	9.3	9.6
Waste			
Count	440	93	533
% within Type of Wrongdoing	82.6	17.4	100.0
% within Type of Observer	48.3	29.7	43.5
Mismanagement			
Count	77	57	134
% within Type of Wrongdoing	57.5	42.5	100.0
% within Type of Observer	8.5	18.2	10.9
Safety problems			
Count	77	23	100
% within Type of Wrongdoing	77.0	23.0	100.0
% within Type of Observer	8.5	7.3	8.2
Sexual harassment			
Count	57	38	95
% within Type of Wrongdoing	60.0	40.0	100.0
% within Type of Observer	6.3	12.1	7.8
Unfair discrimination			
Count	131	27	158
% within Type of Wrongdoing	82.9	17.1	100.0
% within Type of Observer	14.4	8.6	12.9
Other legal violation			
Count	41	46	87
% within Type of Wrongdoing	47.1	52.9	100.0
% within Type of Observer	4.5	14.7	7.1
Total			
Count	911	313	1224
% within Type of Wrongdoing	74.4	25.6	100.0
% within Type of Observer	100.0	100.0	100.0

$X^2 = 89.57$, $df = 6$, $p < .001$

b. Wrongdoing-Type Characteristic Comparative Analysis

After collecting characteristics of each observed wrongdoing type, the researchers explored the cost associated with each, as presented in Table 2 (Table 6 in the source report). The mean cost of all observed wrongdoings was $34,759, with a standard deviation of $40,755. This indicates that large variances exist among the types of wrongdoings observed on the military base. Waste was identified as the most costly of all observed wrongdoings, with a mean cost of $46,694 per incident. Safety problems, with a mean cost of $36,280, were the second-highest cost reported (Near et al., 2004).

The two wrongdoing types with the lowest reported associated costs were unfair discrimination and sexual harassment, with means of $6,673 and $12,826, respectively. This is not surprising, as these types of cost are difficult to associate with a dollar amount.

To determine whether there was a statistical difference between a wrongdoing type and its associated cost, the research performed a post-hoc analysis using the Scheffe test (a method for adjusting significance levels in a linear-regression analysis to account for multiple comparisons). Their analysis indicated that waste was significantly higher in cost than stealing, mismanagement, sexual harassment, or discrimination. As stated above, waste has a higher mean cost per incident than safety problems and other legal violations, but the Scheffe test did not determine the differences to be statistically significant.

The second characteristic captured was the quality of evidence obtained for each wrongdoing type. “Other legal violations” scored the highest overall (with a mean score of 2.81) and was shown to be significantly higher (using the Scheffe test) than stealing, waste, sexual harassment, and discrimination cases. Following close behind other legal violations were mismanagement (with a mean score of 2.30) and safety problems (mean score of 2.08) (Near et al., 2004).

The researchers compared the sum of threatened and actual retaliation to the different types of wrongdoing. The only statistical significance was found in comparing other legal violations to waste. Whistleblowers on other legal violations faced a much

greater level of retaliation (mean of 7.57) than those who blew the whistle on waste (mean of 1.45).

The final characteristic captured was the frequency with which a wrongful activity occurred. As shown in Table 2, there is no significant difference to be drawn between wrongdoing type and frequency of occurrence.

Table 2. Wrongdoing Type Analysis Conclusions (from Near et al., 2004)

Variables	Type of Wrongdoing	N	Mean	Standard Deviation	F	Differs from (a)
Dollar value of activity						
	1. Stealing	102	$ 17,890	$ 30,492		2
	2. Waste	512	$ 46,694	$ 42,161		1,3,5,6
	3. Mismanagement	99	$ 20,379	$ 36,169		2
	4. Safety problems	80	$ 36,280	$ 41,368		5,6
	5. Sexual harassment	40	$ 6,673	$ 21,058		2,4
	6. Unfair discrimination	77	$ 12,826	$ 30,023		2,4
	7. Other legal violations	71	$ 30,871	$ 34,643		
	Total	981	$ 34,759	$ 40,755	**21.75	
High quality of evidence						
	1. Stealing	123	1.91	1.56		7
	2. Waste	548	1.85	1.69		7
	3. Mismanagement	139	2.30	1.60		
	4. Safety problems	106	2.08	1.77		
	5. Sexual harassment	101	1.97	1.46		7
	6. Unfair discrimination	166	1.85	1.50		7
	7. Other legal violations	92	2.81	1.68		1,2,5,6
	Total	1275	2.00	1.65	**5.61	
Frequency with which activity occurred						
	1. Stealing	124	2.44	0.96		
	2. Waste	558	2.33	0.99		
	3. Mismanagement	140	2.53	0.92		
	4. Safety problems	106	2.25	0.94		
	5. Sexual harassment	101	2.36	0.82		
	6. Unfair discrimination	165	2.39	0.73		
	7. Other legal violations	90	2.48	0.81		
	Total	1284	2.37	0.92	1.54	
Sum of threatened and actual retaliation						
	1. Stealing	20	4.40	10.04		
	2. Waste	70	1.45	3.89		7
	3. Mismanagement	45	2.77	6.07		
	4. Safety problems	19	3.52	5.56		
	5. Sexual harassment	23	2.43	3.56		
	6. Unfair discrimination	21	7.23	10.70		
	7. Other legal violations	33	7.57	11.78		2
	Total	231	3.63	7.61	**3.67	

*p<0.01; ** p<0.001

(a)Difference from these types of wrongdoing is significant, p<0.05, based on results of Scheffe test.

The results indicate there is a significant relationship between the type of wrongdoing and whether an observer blew the whistle. The researchers also drew a significant relationship between the type of wrongdoing and the comprehensiveness of relation. However, analysis of the characteristics associated with each wrongdoing type does not paint a clear picture as to why. From this data, one may hypothesize that cost, quality of evidence, and probability of retaliation are the motivational factors that drive the whistleblowing decision.

Wrongdoing pertaining to wastefulness serves as an example. Waste had the highest associated cost implications, the lowest rating for quality of evidence, the lowest comprehensiveness of retaliation, and highest observed instances. Waste was also the one of the least likely wrongdoing types to be reported when observed. This data suggests that lack of quality evidence may lead to nonreporting.

There seems to be a direct correlation between quality of evidence and the probability that an observer will blow the whistle. Other legal violations and mismanagement were the two most-likely wrongdoing types to be reported, and these also carry the two highest ratings for quality of evidence. Sexual-harassment cases were the third-most-likely type to be reported by observers, and ranked fourth on the quality of evidence rating (trailing safety problems by 0.11). It is clear that quality of evidence plays a significant role in the decision process.

The data provided insight as to where government organizations can focus whistleblower-policy efforts. For example, while a constrained budget is one of the greatest concerns for most government organizations and waste and safety violations carry large cost-avoidance potential, these offenses also rank mid to low on probability of being reported.

3. Rewards and Legal Protections

Dozens of federal and hundreds of state statutes provide whistleblowing protections and incentives, including monetary rewards (Feldman & Lobel, 2009). Reform of this legislation is continually undertaken to better incentivize those who step forward and report corporate or government wrongdoings. This section does not review

the legal intricacies of existing laws, but draws from actual cases and the literature to demonstrate how protection laws and monetary rewards may incentivize or frustrate a would-be whistleblower.

a. Monetary Rewards

The best known and arguably most successful tool ever for recovering U.S. taxpayer dollars, with results in the billions, is the FCA. As Senator Charles Grassley, R-IA stated, "We need to send a clear message, from the very top of government, that whistleblowers who expose fraud against the federal government will receive rewards, not reprisals." This is the purpose of the FCA. Under the FCA (since the 1986 amendments), the whistleblower may receive up to 30 percent of any judgment arising from a successful case and is afforded protection from retaliation (Carson, Vedru, & Wokutch, 2007). In fiscal year 2010 alone, over $3 billion was recovered under the FCA, and nearly 80 percent recovered as a direct result of whistleblower lawsuits ("False-Claims Act Overview", n.d.)

In 1987, the Internal Revenue Service (IRS) adopted a similar model that provides financial rewards for those who report tax evasion. Before expanding the Tax Relief and Health Care Act of 2006, the IRS was conservative as to rewards for whistleblowers. Only about 8 percent of whistleblowers were rewarded and the return was only 3–6 percent of total tax-evasion recoveries (Ferzinger & Daniel, 1999). The 2006 amendments provided an alternative mandatory-reward program for actions that exceed $2,000,000 and claims involving individual taxpayers whose income exceeded $200,000 for the year in question (Feldman & Lobel, 2009). For claims that meet these criteria, whistleblowers were guaranteed 15–30 percent of the collected recovery, and a $10 million reward cap was eliminated. By providing enhanced incentives, the number of whistleblower claims exploded from 50 submissions in 2007 to 472 in 2009 (Internal Revenue Service, 2012).

The U.S. Securities and Exchange Commission (SEC) has implemented a similar reward system. Enacted under the Insider Trading and Securities Fraud Act of 1998, it draws upon other models, primarily the IRS's, to increase successful prosecution against

insider trading (Feldman & Lobel, 2009). The SEC made its first award payment under the program in fiscal year 2012. The whistleblower was awarded 30 percent of an approximate $150,000 recovery by the end of the fiscal year (U.S. Securities and Exchange Commission, 2012). As of early 2014, the SEC whistleblower program has rewarded only a single whistleblower a total of nearly $50,000 in the 14 years since the program's initiation. This is partly because, prior to amendments in 2011, the program was poorly incentivized. Reward compensation was capped at 10 percent and limited to penalties imposed under the act (whereas the FCA also permits rewards in *qui tam* lawsuits). Finally, SEC rewards were discretionary and not subject to judicial review, meaning that rewards were not guaranteed even if recovery was successful (Feldman & Lobel, 2009).

b. Intrinsic vs. Extrinsic Motivation

Some experts theorize a downside to monetary rewards. Motivation is commonly defined as intrinsic—stemming from a moral foundation or sense of duty—or extrinsic—motivated by external factors such as rewards (e.g., money) or consequences (e.g., fines). While some argue that extrinsic motivational factors can diminish the intrinsic motivation of an individual, others suggest that the two can be complementary (Bateman & Crant, 2003). The theory of "crowding out," as applied to regulatory incentives, suggests that when people attribute their actions to external rewards and punishments, the moral incentives for their behavior are discounted, thus lowering the power of intrinsic motivation.

In 1999, Edward L. Deci conducted a study examining the effects of extrinsic rewards on intrinsic motivation. Through laboratory experiments, he found that tangible rewards undermine intrinsic motivation for a range of activities (Feldman & Lobel, 2009). As a result of this research, Deci warns that attempts to influence an individual's behavior through the use of external motivation may yield considerable long-term counterproductive results.

To test the impacts of extrinsic, intrinsic, and combined motivational categories, Feldman and Lobel (2009) conducted an experiment with a potential (notional)

whistleblower scenario. Eight survey questionnaires were carefully developed and assigned to eight sub-groups of a sample group. The sample group comprised 2,081 participants who constituted a representative panel based on U.S. census demographics. Each questionnaire contained different motivational and legal mechanisms. All participants were provided the same scenario, as follows:

> Imagine you are an employee of Roadblock LTD, one of the largest construction companies in the country. Roadblock has recently secured a fixed-price government contract to build a major highway in your city.
>
> One day, while staying late in the office, you run across a document that reveals that the company has been substituting lower grade and inferior quality parts from those specified in the contract. The document also reveals that the company has been omitting required testing and quality procedures. You estimate that as a result the government is overpaying your employer approximately $10,000,000 (Feldman & Lobel, 2009, p. 27)

The participants were asked to predict their actions based on the scenario, given the motivational and legal mechanisms provided. The mechanisms were derived from Feldman and Lobel's posited four leading incentive categories for reporting fraud: protection, duty, fine, and reward. The result identified eight categories of motivational/legal mechanisms that correspond to the eight different subgroups. The eight categories developed are as follows:

- High Reward ($1,000,000)
- Low Reward ($1,000)
- Duty + High Reward
- Duty + Low Reward
- Anti-Retaliation Protection (1 Year)
- Duty + Anti-Retaliation Protection
- Duty + Fine ($10,000)
- Duty

Finally, after reviewing the scenario and the motivational/legal mechanism provided, the following variables were measured from each participant:

- Intention of self and others to report
- Evaluation of effect of the motivational/legal mechanism on the decision to report
- Perceived morality, harm, and severity of the misconduct
- Expected social and career ramifications
- Organizational features and individual status

The team found a significant difference among respondents as to how the morality, harm, and severity of the misconduct were perceived. As expected, those who provided the highest scores when judging the scenario as severe and immoral were more likely to report the incident than those who assigned lower scores. To further explore their findings, the research team divided the respondents into two categories: those who judged high severity and immorality and those who judged low. The first group can be considered more intrinsically motivated (high internal) and the second group can be considered as having lower levels of intrinsic motivation (low internal).

The findings show a significant interaction between the type of motivational/legal mechanism and the perceived severity of the misconduct (see Figure 8). For the low-internal group, those in the High-Reward, Duty + High Reward, and Duty + Fine categories were more likely than those in the Low-Reward category to report intent to act on wrongdoing observed. However, in reviewing the high-internal group, there is no significant impact from varying the motivational/legal mechanism. These findings suggest that for those who recognize a moral stake in an issue, external factor variances diminish in significance.

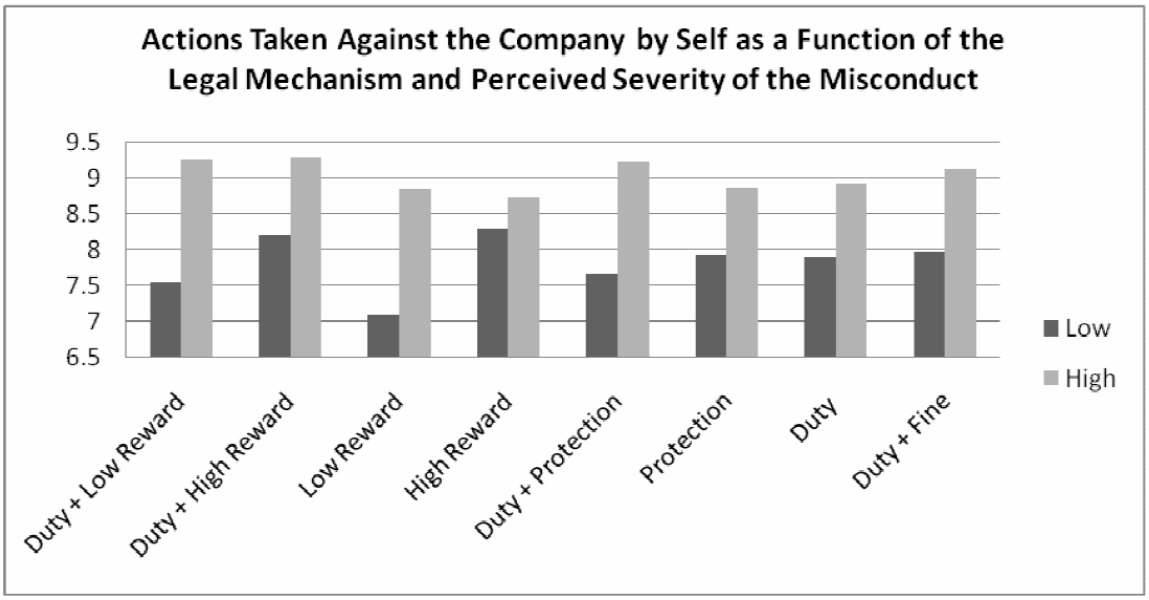

Figure 8. Actions Taken against the Company by Self as a Function of the Legal Mechanism and Perceived Severity of the Misconduct (from Feldman & Lobel, 2009)

The results shown in Figure 1 illuminate the impacts of internal and external motivational/legal mechanisms. External motivations seem to matter much more in the low-internal group. Those least likely to report wrongdoing were the low-internal group when offered a Low Reward. Low-Reward shows the largest variance between the two groups, while High-Reward showed the smallest. These findings suggest a crowding effect, wherein the external motivation seems to have a large impact on the moral dimension of reporting. Another important note is that this variance was less noticeable when examining fines and protections as categories. The researchers conclude that fines and protection as less likely to be perceived as external motivations and less likely to crowd out internal motivations. Finally, the findings suggest that encouraging a sense of duty to report enhances the effect of severity on the whistleblower's intention to inform. Combining duty (an internal motivation) with a high level of external motivation resulted in the highest level of reporting behavior.

c. Legal Protections

The dilemma of the potential whistleblower is between doing right and suffering the consequences, or "swallowing the whistle" and pretending the offense does not exist (Rocha & Kleiner, 2005). Anti-retaliation protections under state and federal law are intended to encourage reporting. This section discusses legislation in a broad sense and assesses the impact protections have on the decision to report.

Anti-retaliation protections have been pieced together from state and federal statutes and common-law exceptions to century-old "at-will" rules. At-will rules enable employers to terminate an employee "for good cause, for no cause, or even morally wrong cause." (Feldman & Lobel, 2009) Over the past 50 years, legislatures have strengthened laws that protect the employee from discharge. Among these is the right to report illegal wrongdoings without fear of retaliation. In the case of Ostrofe v H.S. Crocker Co. (1984), the court ruled that an employee could not be terminated for reporting the legal violations of an employer. The important takeaway was that while there were no anti-retaliation statutes in place, the court nevertheless ruled the case a wrongful termination.

Besides internal and external motivations, Feldman and Lobel's (2009) survey also explored how individuals responded to anti-retaliation protections versus other motivational/legal mechanisms. As seen in Figure 8, the subgroup offered the incentive of anti-retaliation legal protections for a year had an average likelihood of the respondent's blowing the whistle, as compared to other incentives. Not much insight can be drawn from these results, but the researchers went a step further and examined the difference between genders as it applies to whistleblowing incentives.

As seen in Figure 9, women are more likely to blow the whistle than men, overall (Feldman & Lobel, 2009). Gender differences are seen in the motivational factors that protections provide. Women were much more likely to blow the whistle when offered Duty + Protection and Protection than any other mechanism offered. These two mechanisms were also the largest difference between men and women. The important

suggestion from these findings is that men are more likely to be incentivized with a large financial reward, while women care much more about protection from retaliation.

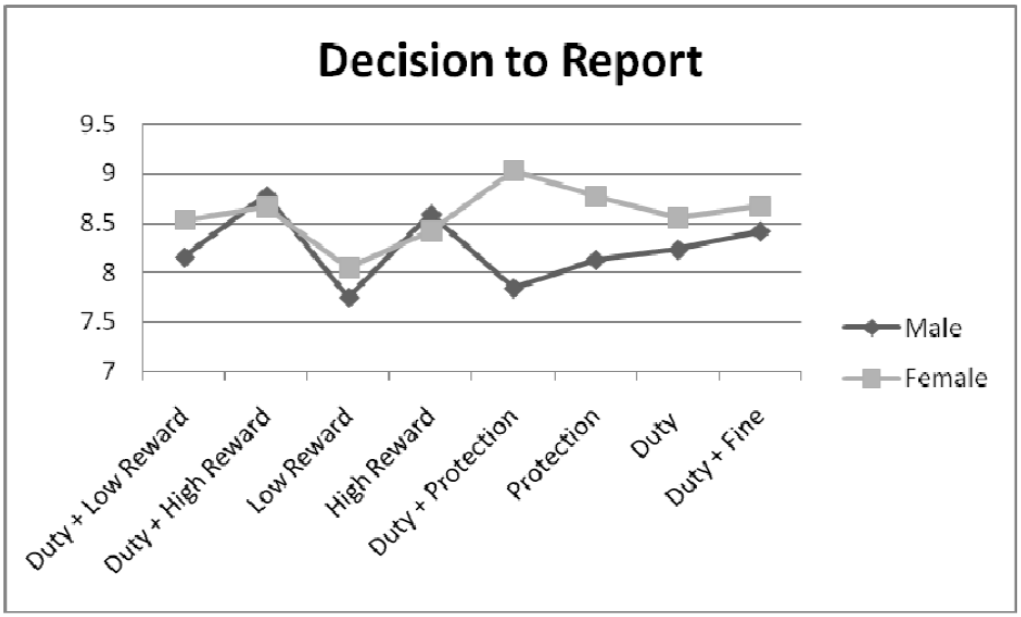

Figure 9. Gender and the Effect of the Alternative incentive Mechanisms (from Feldman & Lobel, 2009)

It can reasonably be assumed that a whistleblower is much more likely to inform knowing that he or she is protected by law against termination, demotion, harassment, and other forms of retaliation. The question arises as to why there was not a higher reporting level for that particular motivational mechanism in Feldman and Lobel's results. One explanation could be that today's whistleblowers assume that protections are automatically granted under the ever-expanding rights of employees. Had the survey clarified that anti-retaliation protection was not covered by the other motivational/legal mechanisms provided, the results may have looked different.

Legal anti-retaliation protections will always factor into the decision-making process. Results show that these protections provide the greatest incentive to women and one of the lowest incentives to men when deciding to report illegal activity in an organization.

B. DISINCENTIVES

Whether or not a whistleblower enjoys legal protections does not mitigate the fact that most people would rather not blow the whistle. As the Army base study by Near, Rehg, Van Scotter, and Miceli (2004) showed, almost three quarters (74 percent) of people who witnessed some type of wrongdoing choose not to report it, a significant number. This section discusses the various reasons that people do not report wrongdoing, including fear of retaliation, rationalization that nothing will be done anyway, the time it takes for a wrongdoing to be exposed, potential delays in receiving financial rewards, and possible negative attention.

1. Retaliation

Through most of the 20th century, employees ideally worked for one company or organization for their entire career, earning their pensions and retiring to a nice life after 30 years. Those days are long past. The U.S. Bureau of Labor Statistics reports (2012) that the average person born in the latter years of the baby boom (1957–1964) held 11.3 jobs from ages 18–46. Employee loyalty to one organization has all but vanished as corporations have merged, manufacturing jobs have diminished, and downsizing or right-sizing have become commonplace. There was commonly an unspoken rule that no matter what an employee saw inside an organization, he would never make it public, even if the activity was unlawful or unethical (Rocha 2005). This expectation of company loyalty has been replaced by loyalty to society (Rocha 2005), whether in terms of environmentalism, public health, or safety issues. As social loyalty increases, witnesses to wrongdoing are more prone to speak out; but with speaking out comes the risk of reprisals, including dismissal, demotion, verbal harassment, shunning, poor appraisals, criminal investigation, job transfer, pressure to keep silent, browbeating over unrelated past offenses, and denial of training or educational opportunities (Devine, 2010; Near et al., 2004). Figure 10 shows the top ten retaliatory measures derived from the Army base study:

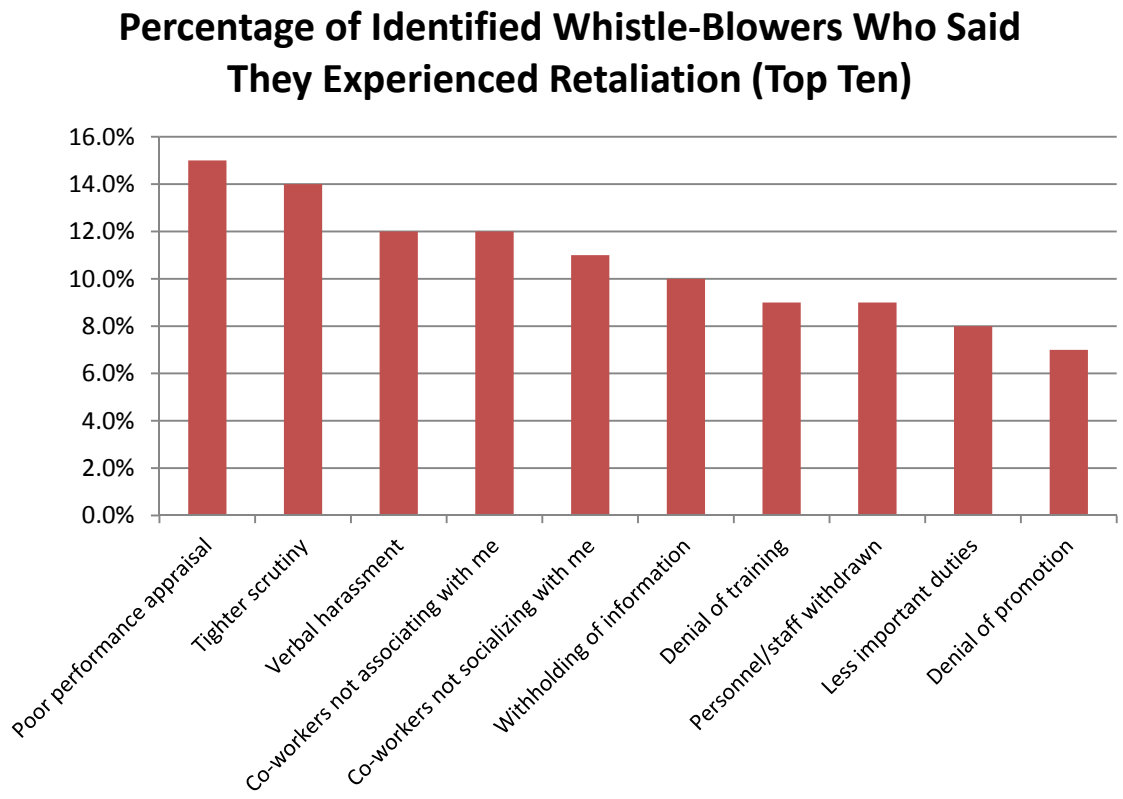

Figure 10. Percentage of Identified Whistleblowers Who Said they Experienced Retaliation (Top Ten) (from Near, Rehg, Van Scotter, & Miceli, 2004)

Retaliatory acts may be motivated by an organization's desire to silence the whistleblower completely, prevent full public exposure of the complaint, discredit the whistleblower, or warn off other potential informers (Mesmer-Magnus & Viswesvaran, 2005). Retaliation does not come from upper management alone. Some supervisors—often without knowledge of upper management—will resort to retaliation to downplay a perceived loss of control in their department or personal influence, or to safeguard their position in the organization (Mesmer-Magnus & Viswesvaran, 2005). Table 3 lists predictors of retaliation as found by Mesmer-Magnus and Viswesvaran (2005).

Table 3. Predictors of Retaliation (from Mesmer-Magnus & Viswesvaran, 2005)

Predictor	More Retaliation Likely	Less Retaliation Likely
Characteristic of Whistleblower	• Older • More valuable to the organization (more loyalty expected) • Values of right and wrong not congruent with the organization	• Younger • It is their job to blow the whistle (e.g., auditor)
Actions Taken by the Whistleblower	• External channels used • Unsuccessfully attempt to remain anonymous	• Internal channels used • Actions are effective in curbing wrongdoing
Contextual Variables	• Lack of support from top management and supervisor	• Coworker support not related to retaliation
Characteristics of Wrongdoing	• Wrongdoing is widespread or organization is dependent upon continuation of wrongdoing	• Multiple incidents, multiple individuals, multiple sources of evidence is unrelated to retaliation

Retaliation often takes the form of damage inflicting on the whistleblower's reputation. The "smokescreen syndrome," as described by Devine (2010,) seeks to discredit the claimant by shifting attention to his motives, professional competence, values, personal life, finances, credibility, or any other vulnerability that may sideline the threat. For example, former Pentagon cost-control expert Ernie Fitzgerald endured repeated personal attacks as his life was probed by then-president Nixon's investigators. More typical is retaliation in the whistleblower's everyday work life, as in the case of Franz Gayl, a lifelong Marine—first as active duty and later as a civil servant—who was instrumental in blowing the whistle on U.S. Marine Corps (USMC) personnel who were not doing all they could to protect their own.

As a science and technology advisor for the USMC in Iraq, Mr. Gayl witnessed deadly attacks on U.S. troops riding in flat-bottomed, high-mobility, multi-purpose

wheeled vehicles, or Humvees. These attacks from improvised, explosive devices (IEDs) led to hundreds of soldier casualties. As early as the mid-1990s, the Marine Corps knew that mine-resistant, ambush-protected (MRAP) vehicles provided at least four or five times more protection from injury or death as did armored Humvees (Gayl, 2009). In early 2005, commanders in the field requested, through an urgent universal-needs statement, an immediate fielding of MRAPs in Iraq. The USMC waited 19 months before finally agreeing to supply the MRAPs—this after a great many soldiers lost their lives in the less-protective Humvees. Mr. Gayl (2009) contends that officials knowingly delayed or refused to provide urgently requested capabilities like MRAP, as the requests competed against preexisting Quantico priorities for other armored vehicles that were known to be vulnerable (Devine, 2010).

Just before his deployment to Iraq in 2006, Mr. Gayl brought the MRAP issue to his chain of command at the Pentagon, reporting that the decision-making process on the urgent request was not getting the attention it deserved. On his return stateside, a meeting was scheduled with the Director, Defense Research and Engineering (DDRE) in the Office of the Secretary of Defense. However, though the DDRE had invited Mr. Gayl to report his findings, the invitation was cancelled by his superiors. Mr. Gayl was barred from any discussion of the problem, as communicated through written correspondence from management that effectively prohibited Mr. Gayl from any "outside communication on the matter" (Devine, 2010). Persisting, Mr. Gayl went to an external source: *USA Today*. After the newspaper published several stories on the delay in fielding the MRAPs, the secretary of defense, Robert Gates, took notice and made the MRAPs the top acquisition priority of the Department of Defense, which eventually ordered and fielded over 10,000 MRAP vehicles.

The *USA Today* stories propelled Mr. Gayl into the limelight. Members of Congress, General David Petraus, the Naval Audit Service (NAS), the Government Accountability Office (GAO), and the Department of Defense Inspector General all wanted to talk with him. These organizations agreed that the USMC had acted too slowly in responding to the IED threat when they had a solution in the form of the MRAP. USMC retaliation was relentless. For sustained periods, Mr. Gayl endured verbal

workplace harassment, assignments with termination threatened if not completed by unreasonable deadlines, and damaging performance evaluations, to name a few (Devine, 2010). Perhaps the strongest retaliation was a 24-month delay in the renewal of Mr. Gayl's security clearance. This came about even as the U.S. Office of Special Counsel blocked discipline on Mr. Gayl for disclosures to the inspector general and Congress, and in fact, obtained agreement for him to submit further disclosures as part of his job duties (Devine, 2010). The USMC searched for ways to find fault with Mr. Gayl in his work and seized upon a technicality when he failed to reference data that was unmarked, but later identified as classified (this was no fault of Mr. Gayl's, as the USMC commanding general in Iraq had marked the material unclassified and approved). Throughout the investigation, the Marines did not disclose information to Mr. Gayl as to any charges, or why he was being investigated. The USMC inflicted further retaliation on Mr. Gayl denying opportunities for continuing education, a Congressional fellowship, and study at the Naval Postgraduate School. Additionally, when Mr. Gayl applied to and was accepted at a prestigious post-secondary university, the USMC denied him attendance, even though he paid for the schooling himself and agreed to be placed on leave without pay for the duration of his studies (Devine, 2010).

The list of retaliations continues. After speaking at the National Whistleblower Assembly (a protected activity), his job description was rewritten, demoting him from a GS-15 to a GS-14. He was reinstated, but only after a key educational activity passed him by, because only GS-15 employees were eligible (Devine, 2010). The Marine Corps opened another investigation of Mr. Gayl through the Naval Criminal Investigative Service (NCIS), which failed to uncover any crimes. However, the probe did find one allegation: Mr. Gayl left a flash drive unattended in a classified area, an area Mr. Gayl's supervisors left unsecured. Without further investigation into this allegation, the Marine Corps suspended his security clearance and placed him on indefinite leave without pay (Devine, 2010).

With such harassment at risk, many potential whistleblowers choose not to get involved. Fear of retaliation is a major disincentive to blowing the whistle, even when it might mean saving innocent lives.

2. Nothing Can or Will Be Done, So Why Report It?

As cited in the Near, Rehg, Van Scotter, and Miceli (2004) study, 74 percent of persons who witness a wrongdoing choose not to report it. Important though fear of retaliation may be as a disincentive, the primary disincentive is less subtle. Of the over 900 respondents who did not report an instance of wrongdoing, over half said the reason was that nothing could or would be done regarding the offense (see Figure 11).

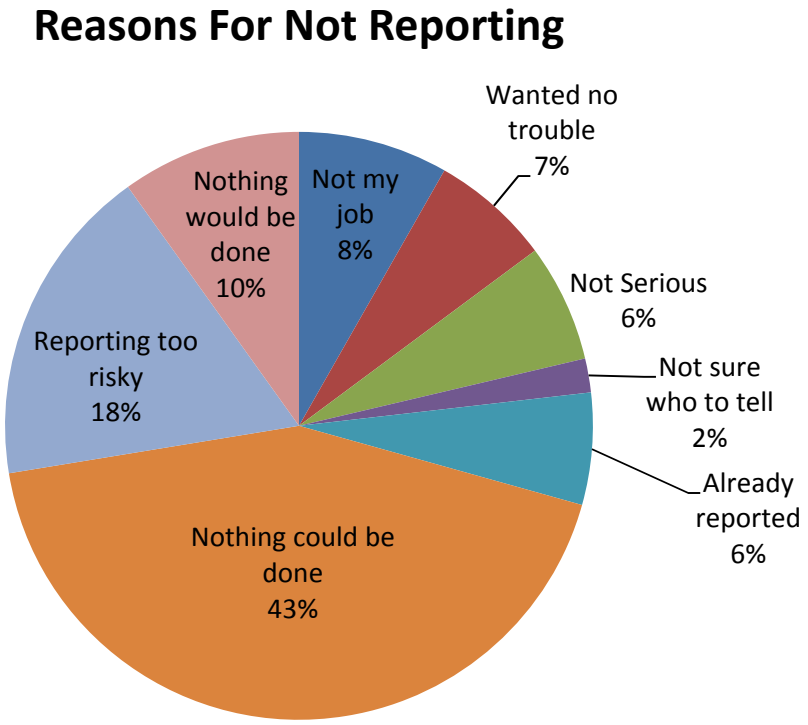

Figure 11. Reasons For Not Reporting Wrongdoing
(from Near, Rehg, Van Scotter, & Miceli, 2004)

Analysis of U.S. Department of Labor Occupational Safety and Health Administration (OSHA) statistics on whistleblower data from FY05–FY12 provides useful data in understanding this disincentive. During that period, OSHA made complaint determinations on over 16,500 whistleblower claims. The number of claims grew slightly from FY05–FY11 (a 1.1 percent growth rate) and then jumped to 42 percent from FY11–

FY12 ("Record Number of Whistleblower Cases Filed," 2013), suggesting that the Whistleblower Protection Enhancement Act of 2012 spurred more reporting.

Statistically, the numbers would imply that the filing of more claims indicates more cases with merit, more recognition accorded to whistleblowers, and more monetary awards paid out ("False-Claims Act Overview", n.d.). OSHA reports each complaint determination in one of five categories: merit, settled, settled–other, dismissed, and withdrawn. Table 4 shows the determination for each complaint and its category.

Table 4. Complaint Determination FY2005–2012
(from U.S. Department of Labor, 2012)

FY	Merit	Settled	Settled-Other	Dismissed	Withdrawn	Total Determinations
2005	41	269	87	1270	235	1902
2006	23	284	117	1275	272	1971
2007	18	261	112	1217	253	1861
2008	21	328	95	1280	296	2020
2009	58	277	116	1218	271	1940
2010	44	309	135	1183	278	1949
2011	55	399	156	1103	300	2013
2012	45	405	187	1665	565	2867
Total	305	2532	1005	10211	2470	16523
%	**1.8%**	15.3%	6.1%	**61.8%**	14.9%	100.0%

Note that while the total number of determinations increased by 42 percent from FY11–FY12, the number of those complaints that had merit decreased by 18 percent. Even more interesting is that, of all whistleblower cases, only a very small percentage were found to have merit and an overwhelming majority were dismissed outright, as presented in Figure 12.

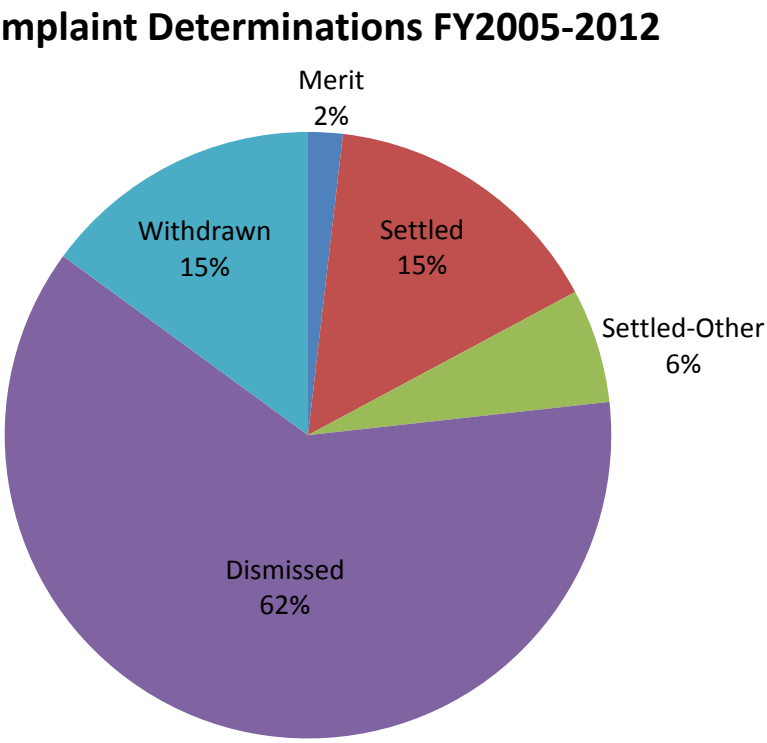

Figure 12. Complaint Determinations FY2005–2012 (after U.S. Department of Labor, 2012)

OSHA frequently trumpets its successes in cases that have merit, when in actuality those cases are the exception, not the rule. When whistleblowers encounter statistics like those in Figure 12, they may become resigned, feeling it is no use reporting a wrongdoing. This research suggests that organizations should consider the data in a different way. If the number of reported wrongdoings skyrocketed in the last year, what is the reason (besides the enactment of the WPEA)—and how can it be used to an organization's advantage? The position promoted in this paper is that organizations can and should work with their employees to secure long-term benefits when a wrongdoing is encountered.

3. A Long, Drawn-out Process

When employees decide to blow the whistle, the decision is not made lightly, since the whole process can take months or years to complete. Many factors contribute to

the time it takes to process a claim. The investigatory process, by its very nature, can be long. There are many variables to consider such as the whistleblower as an individual, the organizational culture, any accusations of reprisals, and the evidence or lack thereof. The realization that it may take a long time to process and investigate a claim could make a whistleblower reluctant to forward accusations, no matter meritorious the claim. To suggest the time commitment, three whistleblower programs in various organizations—the U.S. Military, the SEC, and the IRS—are described below.

a. The U.S. Military

The U.S. Government Accountability Office (GAO) report, "Whistleblower Protection: Actions Needed to Improve DoD's Military Whistleblower Reprisal Program" (2012), observes, "DoD has generally not met statutory requirements to provide reports on completed investigations within 180 days of the date the allegation was made or alternatively, to provide notice to the complainant and the Secretary of Defense," (2012, p. 13). The GAO discovered that although the DoD has made some attempt to shorten investigations, it has not consistently or accurately recorded key dates that would enable it to track how long the process takes to complete (2012). Without this data, the DoD is unable to identify areas for improvement or evaluate the effects of improvements made.

Table 5 shows the speed of the investigative process and percentage of cases in which the DoD misses the mark of 180 days or less.

Table 5. Mean Case-Processing Time by Investigative Phase of Sampled Cases Closed between January 1, 2009 and March 31, 2011 (from U.S. Government Accountability Office, 2012)

Investigative Phase	Number Assessed	Total Days (Mean)	Percentage of Cases Over 180 Days
All cases	91	451 (+/- 94 days)	70% (+/- 11%)
Cases closed before full investigation	61	469	64% (39 of 61 cases)
Full investigation	28	395	82% (23 of 28 cases)

The GAO report reveals that besides failing to complete investigations in 180 days in most cases, the DoD has failed to comply with the statutory reporting requirement by which notification is required for investigations beyond 180 days (2012). Without key timeliness data, the DoD is of course unable to provide chronological information or track and control the process (GAO, 2012). According to the GAO, data recorded in the "DoDIG's (Department of Defense Inspector General's) database understated the amount of days it took to close cases by a mean of 193 days" (GAO, 2012 p. 20). The clock was erroneously started when a clerk was assigned to the case and first opened it, as opposed to when the filer first provided the information to the DoDIG.

Table 6 presents the discrepancy between what the DoDIG recorded in its database and what was actually happening.

Table 6. Timeliness Accuracy by Investigative Phase of Sampled Cases Closed between January 1, 2009 and March 31, 2011 (from U.S. Government Accountability Office, 2012)

Case type	**Number assessed**	**Mean amount of days (DoDIG database)**	**Actual mean amount of days (case file review)**	**Cases with accurately recorded dates in the DoDIG database**
All cases	91	258 (+/- 93 days)	451 (+/- 94 days)	33% (+/- 11%)
Cases closed before full investigation	61	271	469	38% (23 of 61 cases)
Full investigation	28	242	395	25% (7 of 28 cases)

When it takes 75 percent longer to investigate a case than what is officially recorded, it is easy to see why time lags are a disincentive to prospective DoD whistleblowers.

b. Securities and Exchange Commission

Section 21F, "Securities Whistleblower Incentives and Protection," of the Dodd–Frank amendment to the Exchange Act enables the SEC to make monetary awards. An eligible individual must have voluntarily provided original information that led to successful SEC enforcement, resulting in the imposition of monetary sanctions of over $1,000,000 and certain related actions. During FY2012, the SEC made its first award under the whistleblower program (2012). In January 2013, the SEC Inspector General (SECIG) evaluated the SEC's whistleblower program, including a review of promptness in responding to information provided and to award applications and how well the SEC communicated with interested parties (2013).

The data available essentially gives raw numbers, including the average timeline for initial review, the average timeline for initial no-further-action (NFA) determination, the timeline for assigning a point of contact, and the percentage of tips, complaints, and referrals (TCRs) that were designated as NFA or as matters under inquiry (MUI) (SECIG, 2013).

As the SEC provides no analysis to accompany these raw figures and provide context, the SECIG has recommend that performance metrics be developed to determine appropriate response times:

> [T]here is no standard to determine whether the response time is prompt or not. Performance metrics are needed to strengthen the internal controls of the manual triage process. This is needed to ensure consistency in the SEC's processes as new personnel are assigned to the office and as turnover occurs. A lack of performance metrics may result in the degradation of performance and pertinent to this review, unnecessarily long response times to whistleblower information. (SECIG, 2013, p. 17)

Another area in which no performance metrics are present is in the time it takes for SEC Office of the Whistleblower personnel to send an acknowledgment or deficiency letter after a whistleblower submits an application for an award. Since there are no metrics in place, award applications may be delayed; and without a triggering mechanism, these applications may not be resolved in a timely manner. The SECIG concluded that the Office of the Whistleblower should use data collected on its key

performance measures to establish meaningful metrics for the performance of the whistleblower program (SECIG, 2013).

Since the inception of the whistleblower award program two years ago, only two (relatively small) awards have been made, totaling $170,000 (Kelton, 2013). It may be too early to tell whether this unimpressive performance can be attributed to disincentive based on prolongation of the process.

c. Internal Revenue Service

The Internal Revenue Code authorizes the IRS to pay awards for information that leads to the detection and punishment of persons guilty of violating or conspiring to violate IRS laws. The IRS has had the authority to award whistleblowers for many years. In 1996, this ability was expanded, and ten years later, Congress passed the Tax Relief and Health Care Act of 2006, which set limits on awards as a percentage of collected proceeds but did not limit the maximum award payable. The opportunity to receive an award that is limited only as a percentage of collected proceeds resulted in an immediate increase in high-dollar claims submitted to the IRS, some alleging hundreds of millions in tax noncompliance (Treasury Inspector General, 2012). However, with this increased incentivizing of fraud reporting came a backlog of applications, investigations, and rulings, with which the IRS has dealt poorly.

It can take years for an individual's claim to work through the IRS reporting system. The GAO reported that as of April 2011, about 66 percent of claims submitted in the first two years of the program (fiscal years 2007 and 2008) were still in process (2011). After three or four years of filing a claim, two thirds remain in process. The situation may be exacerbated by IRS protocol. The IRS reports that all claims go through a rigorous screening to ensure the integrity of claim reviews and taxpayer examinations. Additionally, taxpayers subject to examination can exercise their rights, which may add years to the process (GAO, 2011). Like the SEC, the IRS does not collect complete data on how long each step in the process takes or the reason a claim is rejected. Thus the IRS is not accountable to any standard by which to measure the program effectiveness. If nothing is measured, there is no way to improve; if there is no way to improve, claims

will continue to remain unresolved for years. The IRS uses the following steps in each whistleblower claim:

1. Filing of whistleblower claim
2. Initial review by whistleblower office (no time standard)
3. Subject-matter-expert review (no time standard)
4. Classification and examination
5. Appeals and collections
6. Period for taxpayer to exercise right to request refund
7. Whistleblower office final review
8. Award payment

Both the Treasury Department IG report and the GAO report note that communications on whistleblower claims need to improve within and without the organization, as well as timeliness of resolution. The timeliness standards established by the IRS were adjudged as failing to provide uniform guidance in the processing of claims (Treasury Inspector General, 2012). For some reason, the IRS finds it difficult to include data on how long it takes to process whistleblower claims. In their 2010 annual report, the IRS gave the number of whistleblower claims and number of taxpayers those claims identified, but not data on the time required for claims to process or any specific information on rejected claims (2010). This lack of data limits Congress's ability to oversee the program. Additional data could improve program transparency and encourage whistleblowers to come forward (GAO, 2011).

It appears the IRS may be turning things around. Whereas in 2011 the first award was made on a claim first filed in 2006, late in 2012, several high-profile awards were announced (Jones, 2012). Possibly because of the Treasury IG and GAO reports, the IRS has implemented the following guidelines (IRS, 2013):

- Claims should be initially evaluated by the whistleblower office within 90 days.
- Review by experts in IRS operating divisions and criminal investigation should be completed within 90 days of receipt from the whistleblower office.
- Whistleblowers should be notified of an award decision within 60 days of when collected proceeds can be determined.

Despite this progress, waiting three, four, or even five years to collect on a claim can be a discouraging prospect. As yet another example disincentive, the IRS enforces 28 percent tax withholding on all program awards (Saunders, 2014). This tax is exactly the opposite of what is needed to get witnesses to speak up when someone tries to circumvent the nation's tax laws.

THIS PAGE INTENTIONALLY LEFT BLANK

V. ANALYSIS

Systems theory has proven an effective model for assessing organizational behavior (Millett, 1998). By treating an organization as a system, an analyst can discover complexities and subsystem connections that affect how the organization operates. In this chapter, the effects of having an established whistleblower policy (including training and processes) is analyzed, using an open-systems perspective model.

A. OPEN-SYSTEM ORGANIZATIONAL-MODEL ANALYSIS

Under a systems view, an organization is assessed as a set of interacting functions or subsystems that acquire inputs from the environment, transform them, and release them as outputs back to the external environment (Draft, 2001). An open-systems perspective views organizations as complex organisms that "live" in an external environment (McShane & Von Glinow, 2012). In other words, the system (or organization) is significantly influenced by its external environment, with which it exchanges inputs and outputs, both good and bad. This section explores how whistleblowing can affect an organization's external environment, how that environment affects the organization, and as part of sound organizational design, a good whistleblowing policy and process can help an organization maintain equilibrium—that is, a healthy, normally operating, efficient state of being.

In exploring whistleblowing within the government, evaluating the organization in question as an open-systems model can provide valuable insights. The starting assumption is that the external variables play a significant role in explaining what happens internally (Allen & Sawhney, 2010). Human organizations are normally described as "open" systems. Whereas closed systems have clear boundaries that define them regardless of external influences, the boundaries of open systems are permeable (Millet, 1998). A clock is a good example of a closed system: regardless of what else is happening, it continues to perform as designed. A government organization is much more complex and greatly influenced by surrounding government—thus an open-systems model is the logical choice for this research.

1. Organizational Model Description

In assessing a government organization as an open system, a model developed by the Breckenridge Institute is useful in providing a graphic display of the organization as a starting point. The model version used in this research is customized slightly to demonstrate some key points. The following section describes the elements of the open-systems model, as defined by the Breckenridge Institute (Breckenridge Institute, 2013).

Figure 13 displays the structures and systems of an organization as a process-oriented system that operates within an organizational climate or culture and influences, or is influenced, by the external environment, on which it depends for survival. According to the Breckenridge Institute,

> On the open systems view, organizations are like organic, living, goal-seeking organisms where their structures and systems reach a state of equilibrium within context of their internal climate and the forces and pressures from business environment outside the organization (Breckenridge Institute, 2013).

This idea of constantly seeking to reach or maintain equilibrium is key, as is the notion that everything within an organizational model is connected.

There are three main elements in the organizational model in this research: strategic view, execution, and organizational climate. The strategic view defines the overall direction, goals, and objectives of an organization, and is a critical element of any organization. Inputs from the environment need to be interpreted and plans need to be established to execute organizational actions within an organizational climate. Note that the output from the strategic-view element sets the stage for the climate and execution elements of the organization.

The elements necessary to execute a strategic view are reflected in the execution perspective. Within this view, all elements (decisions, people, processes, rewards, information, and structure) are interconnected. For example, having a formalized structure enables people to execute processes, make informed decisions, and be motivated by some sort of a reward.

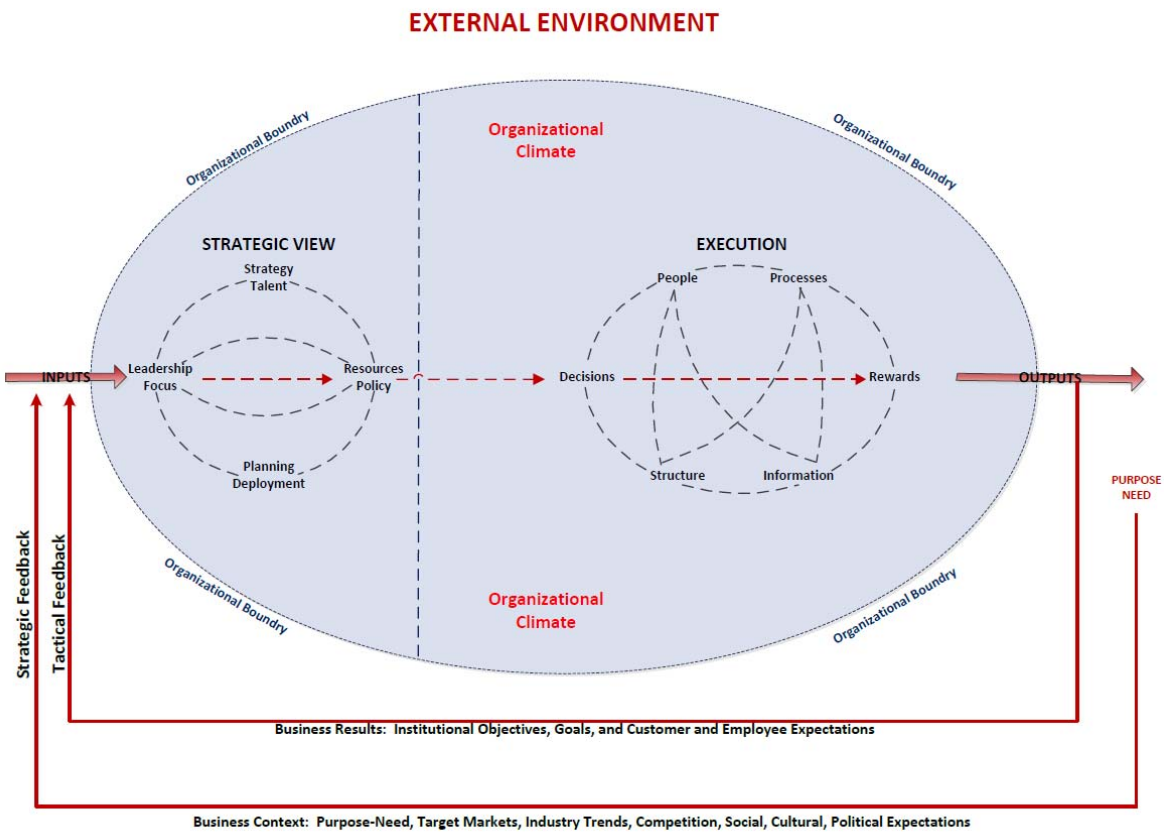

Figure 13. Breckenridge Institute Open Systems Organizational Model (from Breckenridge Institute, 2013)

The final main element of the organizational model is the organizational climate. Loosely speaking, organizational climate is the experience of an employee on a day-to-day basis, consisting of the underlying cultural norms of an organization. A good organizational climate is instrumental to higher employee satisfaction, better interpersonal relationships, and, as a consequence, higher productivity (Sahni & Kumar, 2012). An organization's climate is depicted as existing within the organizational boundary, but influenced by the external environment.

Another key element in the open-systems model is the organizational boundary, or what separates thane organization from other social entities. These boundaries can take many shapes and forms, including the physical (e.g., a building or location), time-related (work shifts or time zones), social (hierarchies and discipline), language (industrial or national), and cultural (shared beliefs, values, and stereotypes). Organizational

boundaries in an open-systems model are permeable to the external environment. The degree of permeability is important for controlling forces from the external environment and enabling the organization to reach equilibrium. Control must be deliberately designed and monitored by leadership.

The external environment is quite simply, everything outside the organizational boundary. An organization must interact with the external environment to survive. Customers, suppliers, and competitors are three common external elements that directly influence an organization. Much of the information available in the external environment is irrelevant to the organization and provides no added value; thus, inputs must be filtered by management. While every organization receives external inputs and returns outputs, it is important to understand that the external environment can be influenced, but not controlled.

All organizations have a purpose or need to exist. To survive, an organization must align its vision and goals with tangible needs that occur in the external environment, and the organization's purpose becomes meeting these needs. The output (or strategic plan) from the strategic view in Figure 13 should guide the organization toward fulfilling its purpose in the external environment.

The open-systems model provides two feedback loops: the tactical and strategic. Tactical feedback can be thought of as business results. It describes how well an organization is meeting its defined goals by measuring the results produced (financial and otherwise). Strategic feedback, on the other hand, indicates how well the organization is aligned with its purpose of meeting needs in the external environment.

2. Whistleblowing-Event Analysis without Internal Policy

For demonstration purposes, a governmental acquisition organization is assessed below, in which a whistleblower event occurs. It is assumed that the organization has no internal policy for reporting fraud or observed wrongdoings. To analyze the whistleblowing event from an open-systems perspective, we explore the actual experience of an employee in the execution section of the organizational model. As

shown in Figure 14, the output generated by the organization does not follow its designed path.

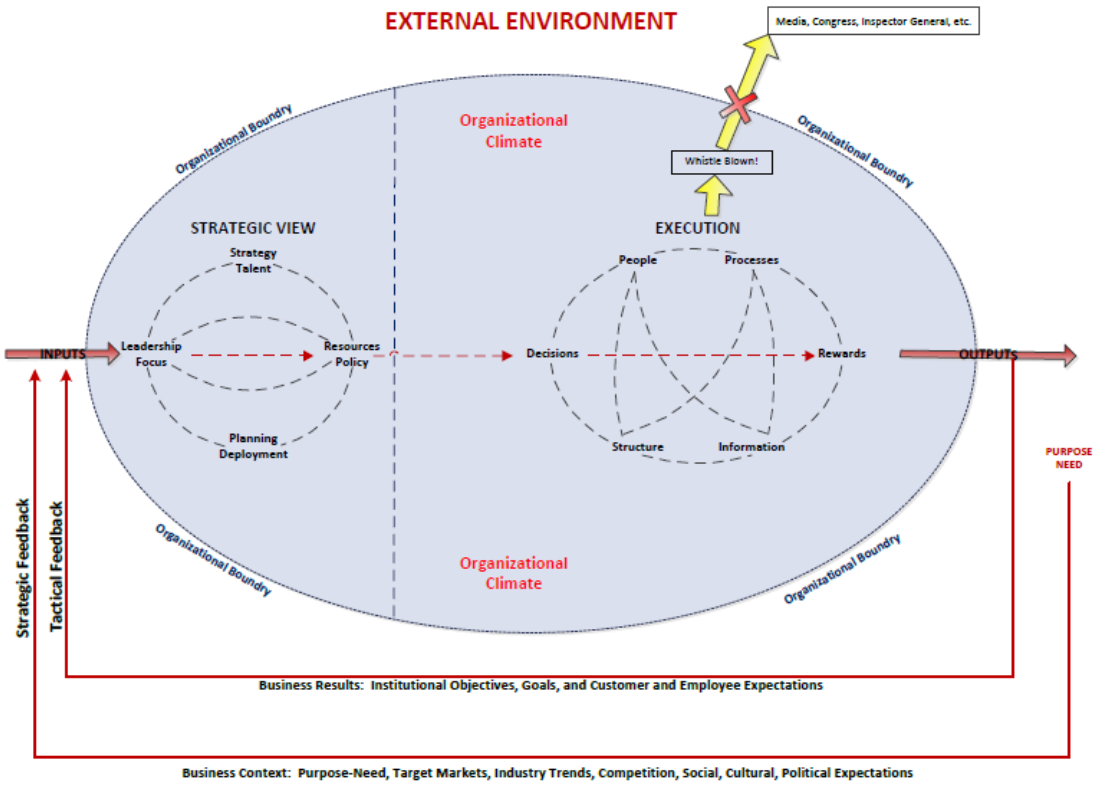

Figure 14. Open-Systems Organizational Model (after Breckenridge Institute, 2013) Whistleblowing Event without Internal Policy

In an uncontrolled external whistleblowing event, the flow of information across the organizational boundary to the external environment (output) is outside the organization's control. As often seen in whistleblowing cases, the individual(s) went directly to the external environment to report a wrongdoing in lieu of following policy and process. This action signals a breakdown of organizational design. The organizational boundary is permeable from an open-systems perspective, but the border must be controlled for an organization to reach equilibrium and efficient performance. Before examining the effect a whistleblowing can have on an organization, let us first

explore the organizational-design problems that may have allowed the uncontrolled situation in the first place.

Upon further examination of the organization's execution element, several interconnected sub-elements are revealed: decisions, people, structure, processes, information, and rewards. In this model, it is easy to visualize how organizational decisions can impact the structure and the persons within it. If no decision was ever made to design and promote a whistleblower program, there may be no structure to support such an activity, nor would the right people be in positioned to develop, sustain, and act upon it. Thus the cascading impacts of each single sub-element are apparent. Without a supportive structure for whistleblowing, the processes needed to empower a would-be whistleblower would not exist, information would not be communicated (e.g., through training), and of course, there would be no reward as an incentive. Every decision sub-element is therefore equally critical—carrying equal weight, they together constitute the execution element as a whole.

The precursor to the execution element is the strategic view in the open-systems model. The strategic view, developed by leadership, establishes overall direction and sets the stage for how an organization executes in its external environment. In this example, whistleblowing was not captured at a strategic level, hence not captured as a leadership focus area. Therefore, no policy was developed to support its execution. It becomes easy to see how the execution element spun out of control in the whistleblowing event. Without the strategic foresight to anticipate (or encourage) and manage such an event, the employee is more likely to create unmanageable outputs to the external environment.

Now let us explore the external environment of the open-systems model before an external whistleblowing event. In an open system, inputs are received as tactical and strategic feedback. In this example, we focus on strategic feedback, which is described as business context. Leaders must understand the social, cultural, and political expectations of the organization and develop a strategic view to accommodate them. A government organization in the United States is entrusted with taxpayer money. American taxpayers make up an extremely large community of stakeholders; therefore, it is critical to exercise

good stewardship of taxpayer funds if the organization means to stay intact and provide a service to the country.

In the example provided, an external whistleblowing event caused an uncontrolled output to the external environment. Let us return to a case previously referenced, wherein Mr. Gayl blew the whistle by going direct to *USA Today*. In today's society, the media is a critical component of the external environment, with which communication must be controlled. Mr. Gayl's uncontrolled external output created severe unwanted consequences for the USMC. This resulted in new inputs, which shifted the organization's attention from its primary mission to managing increased media attention, congressional oversight and testimonies, litigation, and mistrust from key stakeholders.

3. Whistleblowing-Event Analysis with a Designed Internal Policy

An organization with a deliberate organizational design to address or encourage whistleblowing is in a much better position of control. As noted, controlling information flow between an organizational boundary and the external environment is critical to operating with any sort of efficiency.

As organizations draw inputs from the external environment to operate, they also create outputs to the external environment, which creates a feedback loop. As a central-control mechanism for maintaining balance between order and chaos (Millett, 1998), the feedback loop becomes an input to strategy and execution. As demonstrated in Figure 14, an organization without a deliberate whistleblowing policy can lose control, and the ensuing chaos may decrease operational effectiveness.

All government organizations have many inputs from the external environment, but this analysis focuses specifically on social, cultural, and political expectations and the strategies that ensure these expectations are met. Good stewardship of taxpayer money is one key expectation. Because fraud is everywhere, a government organization must have means to identify and address wrongdoing to fulfill its stewardship function.

Once an input is understood, it needs to be interpreted within the strategic view of the organizational model (reference Figure 13). Senior leaders of the organization

understand that fraud can happen; thus they must be prepared to handle it. This realization creates leadership focus, which enables the development of policies to address whistleblowing, allocates resources in support of policy development, and identifies the strategic talent required. Finally, plans for deploying the policy are made. All the elements identified in the strategic view must be addressed to enable successful management of a potential whistleblowing event.

Once a strategic view is established, it must be communicated to enable the execution element of the organizational model. For successful management of potential whistleblowing events, each sub-element must be addressed and assessed for interactions. Most organizational decisions are delegated to managers at lower levels than those who establish the strategic direction. Again, the sub-elements should direct these decisions towards a common goal of finding ways to manage whistleblowing events and maintain control. These lower-level decisions will affect how structure and processes are developed to report, monitor, and control whistleblowing cases. When developing process and structure, leaders must also understand what type of reward (incentive) will appeal to employees within the organization. The final step is to provide the required information to all personnel as to how whistleblowing can and will be received.

Applying systems theory, utilizing an open systems model of an organization, offers many insights into organizational behavior during a whistleblowing event. Organizational leadership can use this as a tool to assess the complexities of the many interconnected subsystems within the organizational boundary. By doing do so, adjustments can be made to address gaps in the strategic or execution areas of the organization to effectively enable and control whistleblowing events.

VI. CONCLUSIONS/RECOMMENDATIONS

A. A DELIBERATE/TAILORED WHISTLEBLOWING POLICY

Wherever the fraud triangle of pressure, opportunity, and rationalization exists, fraud will happen. There are several institutional vehicles for reporting fraud, including audits, the Defense Contract Management Agency, Federal Acquisition Regulations, and inspector-general investigations. One of the most valuable methods, though infrequently captured by program managers, is whistleblowing (Pierson, Forcht, & Bauman). PMs can use information provided by internal employees to make their organizations more efficient, transparent, and financially and ethically sound, and to yield a better workplace overall.

To secure these results, PMs must adopt an attitude of openness, address and investigate allegations of wrongdoing, correct bad policies, depersonalize the process, and implement an internal whistleblowing program for the benefit of the employee and organization. The following recommendations require changes in the organizational model, including an internal-feedback loop and an external-output mechanism. Finally, a strategy on how to implement and execute a deliberate whistleblowing strategy is presented.

B. ORGANIZATIONAL-MODEL RECOMMENDATIONS

To develop a whistleblowing policy for a program office, this research recommends beginning with an open-system organizational model such as that of the Breckenridge Institute. Graphically displaying the interconnected subsystems within the organization is a first step to ensuring that all required connections and interdependencies are acknowledged and addressed.

Two alterations to the organizational model are recommended. First and most important is implementation of an internal-feedback loop; second is an external-output mechanism for would-be whistleblowers, to avoid uncontrolled release of information to the external environment.

1. The Internal-Feedback Loop

An internal-feedback loop from execution to the strategic-view element, as shown in Figure 15, will essentially inform senior leaders as to how the organization is executing their strategy before generating outputs to the external environment. Internal-feedback loops give several benefits. First, they are essential control mechanisms, allowing leaders to assess how well the whistleblower policy is working, adjust strategy if necessary, and intervene in the execution element if something appears to be broken. Second, internal-feedback loops foster a healthy organizational climate. By listening to employee feedback and actively ensuring that strategy is aligned with personnel needs, leaders improve organizational climate; if employees are trust that their senior leaders will fully support the whistleblowing policy, they are much more apt to feel they can make a difference and more likely to report wrongdoing. Overcoming any perception that "nothing could be done about it" is critical, as a sense of pessimism is the primary reason offenses go unreported. The emplacement of an internal-feedback loop encourages employee confidence in leadership commitment to follow-through and openness to change.

While incorporation of an internal-feedback loop offers better control and may improve the organizational climate, it does not cover the organization's entire need. When senior leadership is accused of a wrongdoing or ignoring a problem, the whistleblower must have ways to report the issue to the external environment, but via a controlled process in which the organization isn't thrown out of equilibrium.

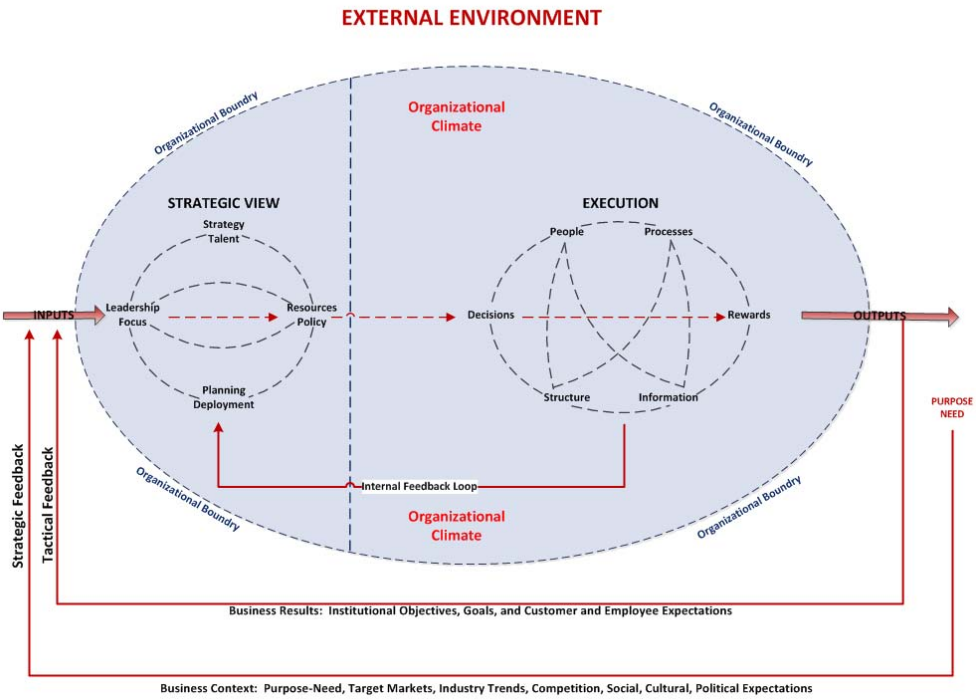

Figure 15. Open Systems Organizational Model (after Breckenridge Institute, 2013) with Internal-Feedback Loop

2. Controlled External-Output Mechanism

As seen in the example of whistleblower Franz Gayl, an uncontrolled external output created severe and unwanted consequences for the USMC. Mr. Gayl attempted several times to report to his chain of command (an internal process) and his motions were dismissed by his superiors. When a whistleblower is rebuffed, he has two options. He may drop the issue, like the 74 percent of employees cited above (Near et al., 2004), or he may bypass the chain of command and present his case to receptive parties in the external environment. Mr. Gayl chose to bypass the chain of command, but had no external process to follow. He therefore took it upon himself to report the observed wrongdoing to *USA Today*.

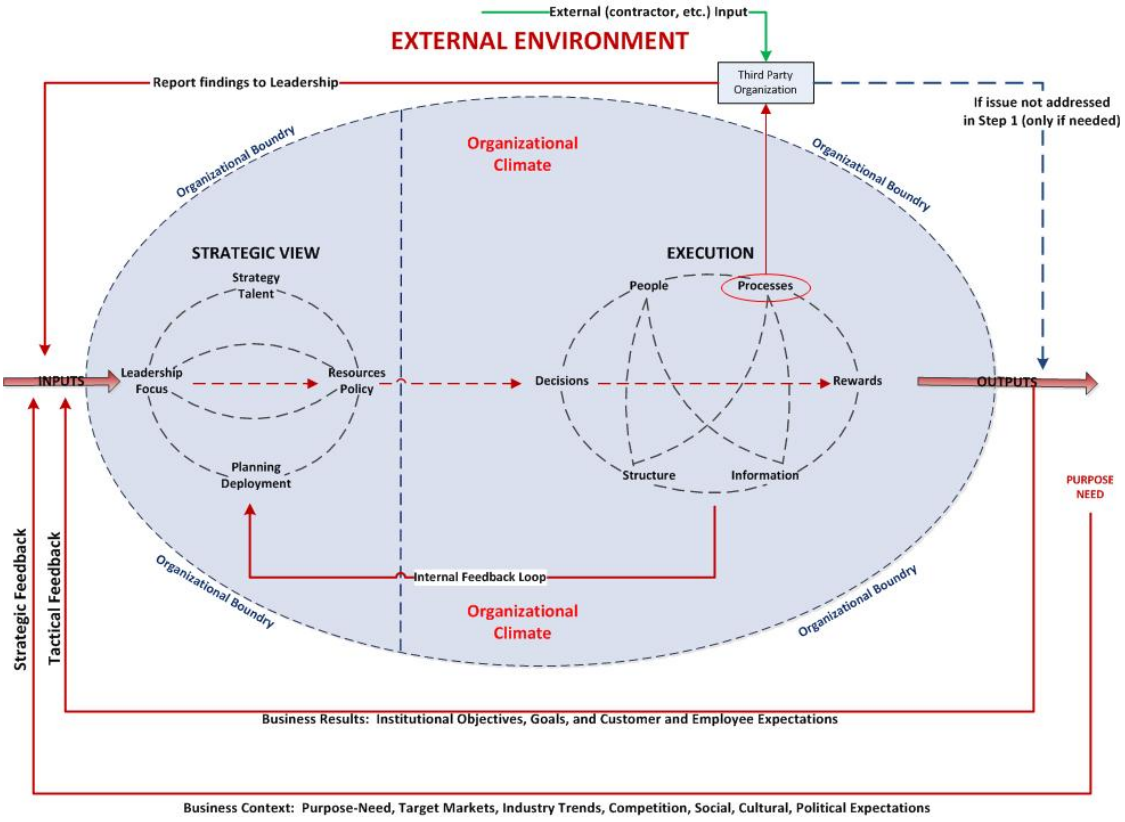

Figure 16. Open-Systems Organizational Model (after Breckenridge Institute, 2013) with Internal-Feedback Loop and Controlled-External Output

To avoid such uncontrolled external reporting, it is recommended that program managers develop a way for would-be whistleblowers to bypass their chain of command if needed. The organization should contract with a third party to collect whistleblowing outputs and relevant information and provide a feedback loop to organizational leadership. Figure 16 displays how a third party can collect organizational output and provide feedback (represented by a red arrow) as an input. The purpose of this design is to allow a prospective whistleblower to bypass chain of command, remain anonymous if desired, and still notify the PM leadership team of alleged fraud or wrongdoing. This gives organizational leadership—not just one person, but all key leaders—the ability to investigate, mitigate risks, find a solution, and prepare for consequences if and when the information goes public.

In the event leaders disregard the reported fraud or wrongdoing, the third party should have means to take its findings directly to the external environment (represented by the dotted blue line in Figure 16), and the PM office must provide clear and concise criteria under which the third party is authorized to do so. This mechanism is crucial to ensuring the integrity of the policy when management itself is the alleged culprit.

Another key benefit to using a third party is that it can collect inputs from the external environment for the PM office (represented by the green line in Figure 16). These external whistleblowing inputs could come from service organizations, defense contractors, or any other channel outside the PM office and be collected, organized, and communicated via the feedback loop to organizational leaders for further action.

The proposed changes in organizational design are intended to control the external output of fraud or wrongdoing and thus enable leadership to eliminate or correct the risk internally, with minimal damage to the organization. To accomplish an effective whistleblowing policy, the PM office must focus on the strategic and executional views of the organization.

C. STRATEGY

One prerequisite in the development of an internal whistleblowing strategy is strong endorsement from upper management. Employee awareness and empowerment rises when leaders take a strong stance on whistleblowing, implementing a conducive strategy from the top down and promulgating it throughout the organization. A written whistleblower policy is vital. PMs must produce a formal policy with a well defined role and purpose, containing clear information on what should be reported, how it should be reported, and to whom. One or more mechanisms must be provided by which employees can report offenses—for example, an independent third party to hear complaints or a senior-level champion in charge of the program. Potential mechanisms are described further below.

1. Leadership Focus

The ethics and culture of an organization flow from the top down and are revealed through policies, procedures, and the example set by executive officers. A clear connection needs to exist between an organization's code of ethics and its performance measures. Leaders need to treat whistleblowing as the moral obligation of everyone, from CEO to new intern, and PMs need to cultivate an environment where downward and upward communication is encouraged. The open-door message must be promoted by program managers and supervisors at all levels. Individuals will more likely take advantage of whistleblowing mechanisms if they know their voices will be heard. The PM must affirm his commitment to the whistleblowing policy whenever appropriate and publically acknowledge and reward employees who raise ethical concerns (subject to their permission). Program managers must also clearly communicate to subordinates the following information:

- The program manager's overall stance on fraud
- Examples of what fraud is
- How fraud can harm the organization
- The importance of reporting suspected improprieties
- How to make a report
- The necessity of ensuring anonymity
- What happens after a report is made
- What to do if a supervisor or senior leader is suspected
- Assurance that all reports will be considered seriously and investigated promptly

The latter point is very significant to employees, who are typically anxious that allegations be investigated thoroughly yet quickly. They must also feel confident that any results from the investigation will be reported by their immediate supervisors to a higher authority.

Many reports of fraud come from outside the program manager's office; accordingly, vendors, contractors, and employees of other DoD agencies should also be

made aware of whistleblowing policies. Readily available, effective training will enable employees to identify exactly what fraud is, how to recognize it, and how to report it.

2. Policy Development

An organization's commitment to whistleblowing is set forth in its formal policy. The PM's fraud-reporting program should have a clearly defined scope and purpose, and controls and procedures for processing allegations must be clearly understood. The very existence of a formal policy signals to employees that eliminating fraud is an important goal of the organization and instills confidence that whistleblower information will be handled well. The policy serves as a reference guide, describing how the system works, the roles and responsibilities of each person in the process, how reports are assessed, how investigations proceed, what happens after an investigation, and the kinds of protections in place. At minimum, the following definitions must be clear:

1) What is a whistleblower

2) The type of fraud to report

3) Protections available to the whistleblower

The policy must also list clear steps for reporting wrongdoing and specifically indicate who handles whistleblower complaints, with the role and responsibilities of this party.

This research recommends that an external, independent party be contracted to receive information. A third party can offer expertise not usually available internally, allay whistleblower anxiety, and receive external output in a way that will not damage the institution. A controlled external-output mechanism, whether a tipster hotline, website, walk-in office, or mailing address, both encourages the whistleblower and benefits top management by providing a way to learn of the alleged problem, investigate, and prepare to deal with the outcome.

A good policy should also specify a person charged to look after the welfare of the whistleblower. Reprisals from colleagues or middle management can occur even in

organizations with strong whistleblower policies. If employees know that top management will shield them, they may feel more comfortable coming forward.

A whistleblower policy should explain how fraud data is collected, reported, and stored within the organization. This data should never contain elements that might compromise confidentiality; few employees would speak out, especially with serious allegations, if information were not held extremely close.

How an investigation is conducted, who is involved, and actions taken after the investigation are of great interest to potential reporters, and should be detailed in the formal policy. The whistleblower also needs to see how he will be kept informed and what to do if adverse action is taken or if he himself is accused of wrongdoing. The accused employee is also an important party in a whistleblowing scenario, and the policy must also cover how his rights are protected, including the right to know what is being investigated, to respond to allegations, and to protect his identity.

3. Resources

A whistleblower policy may be all encompassing and every aspect of the program may be documented, but that does not guarantee smooth implementation. Along with top-management commitment and a well-considered policy is a need for resources to implement the policy and create a reward structure.

Just as a weapon system needs dollars for personnel, hardware, training, and sustainment, a whistleblower program requires financial support from program managers. The PM's program is an investment that will pay off as illegal and fraudulent acts are reported —but there are up-front and continuing costs.

The resources needed include, in the first place, personnel to write a comprehensive policy. The PM may be able to use the human-resource department, though many times he must pay for this matrix resource. In addition, costs such as training and setting up reporting vehicles must be accommodated.

A program manager often has little latitude to divert funding towards a reward system for whistleblowers. In the FCA, IRS, and SEC whistleblower programs, rewards

are paid from funds collected through enforcement; while PMs should be aware of these programs and provide information to all potential whistleblowers, there are other ways to reward an individual that may be within the PM's power.

D. EXECUTION

Once management has developed a whistleblowing strategy, it is time to execute it. Here all the elements of fraud management come into play: preventive, detective and corrective controls over the five primary considerations (process, people, decisions, information, and rewards) to reduce the fraud triangle of pressure, opportunity, and rationalization.

1. Process

It is vital that the whistleblowing process not be seen by the workforce as an added burden on their duties. Using a third party as recommended will keep staff time commitments to a minimum. The third party should conduct audits of every PM process to ensure that employees are working correctly and honestly. As a vital part of detective control, these external audits should happen by surprise, to give fraudsters less chance to hide their actions and auditors more chance to discover them. Surprise audits are also a preventive control, providing disincentive and helping reduce opportunity. Besides external audits, internal audits by a team of handpicked representatives from every major process in the organization should be held. Senior leadership should provide enough resources and authority to the team that they are taken seriously and can operate without intervention from the top. Auditing software may be used to supplement the audits, especially in financial areas. The use of such software should be known to the workforce so it can function as a deterrent–but it should be run and maintained by a third party to keep its operation opaque. The auditing software should be included in policy development and testing as a good way to identify vulnerabilities to internal or external fraud.

The PM should maintain a proper separation of duties among employees to reduce perceived opportunities to commit fraud. Thus, the person receiving and verifying purchases should not be the same as the person who approves or places the order. The

financial team should be structured so that one person's work double-checks another's. No single person should have access or authority to complete a financial transaction alone, nor should the person conducting an inventory of PM-owned assets be responsible for their safekeeping and operational use.

The process must provide potential whistleblowers with options. Every individual should potentially feel comfortable with at least one way of providing tips, whether directly, through a supervisor, externally, through a third-party partner, or through a website—with anonymity always a clear option.

All tips should be investigated quickly and the results should be available to the workforce. The fraud prevention and whistleblower process will be significantly more effective if the workforce receives regular feedback and updates on the process. To catch trends that may reveal systemic problems, a database should be created.

2. People

The PM should keep employees invested, from training to outcomes. As noted, upper management must set the proper climate and tone at the top. Employees should not only hear their leaders condemn fraud, they must see honesty and integrity in action. Fraud-policy communications should be sent to the workforce directly from upper management, and management should present fraud information on a monthly basis.

To reduce the pressure side of the fraud triangle, management should set realistic work-performance goals for employees—they should be challenged to excel, but not stretched to the breaking point. Unachievable goals lead to bitterness and overworked employees become stressed, never receive the satisfaction of meeting goals, and endure gratuitous pressure. As a preventative, employees should be encouraged to use their annual leave to reduce stress levels and coworkers should be cross-trained to handle the responsibilities of employees on leave, so as to prevent their stressful return. Cross-training allows an organization to run efficiently in case of sickness or other absence as well and, key to issues of fraud, makes coworkers familiar with normal behavior, processes, and actions in other areas within the PM. Something out of the ordinary can thus be more readily identified and brought to a supervisor's attention.

A healthy work environment conduces to happy, relaxed employees; but there is always the possibility that the personal circumstances of an employee may become a source of major stress. The PM should be cognizant of behavioral changes in employees and recognize destructive behaviors. For issues of addiction, mental and emotional health, family problems, or financial issues, the PM should be versed in the range of state and federal support programs that may be available and encourage him to seek help, offering mentoring as appropriate.

The PM should arrange independent, anonymous, third-party surveys to determine the extent to which employees feel management acts honestly and responsibly. The survey should capture employee morale and solicit suggestions on improving morale. Management should review these surveys and provide a summary, along with a list of actions taken to address identified concerns.

Fraud-prevention goals should be incorporated into a manager's annual performance goals to expedite progress and demonstrate upper leadership's commitment to fraud prevention. Managers must operate under a true open-door policy, so that employees feel comfortable approaching their supervisors with concerns and feelings of pressure. This allows management to deal with difficulties in their infant stage, before they grow and possibly spread within the organization.

3. Decisions

The need for decision making comes into play primarily in the area of corrective controls. Once a fraud has been reported or a fraudster identified, the PM needs to decide how to handle the situation. Since fraud takes many forms, from foisting of unsafe military equipment to siphoning of millions of dollars, the PM must determine individually how best to handle each case.

The PM must not be ashamed, timid, or complacent when dealing with fraudsters. The PM must show zero tolerance towards fraud and set the right tone by acting in an official capacity and involving outside authorities. If the fraudster worked within the organization, he should be removed. Law enforcement should be informed, civil action

should be taken, and regulatory authorities should be notified. A slap on the wrist or, worse, no action at all, sends a cynical message that defeats the concept of zero tolerance.

When there is no conclusive evidence of fraud, a formal written warning or reprimand should be given, or both. A note should be made in the employee's permanent record, which will provide background should another allegation be made. If the fraudster works outside the organization, the PM should cease involvement with any business or organization he is associated with.

The PM will not necessarily have, and should not pretend to have, legal authority to handle all the issues that whistleblowers may bring to light. Thus the importance of retaining a third-party organization to handle cases beyond the PM's domain, in which federal or state organizations must be invoked.

4. Information

Having designed an outstanding whistleblower policy and supported it with resources, the PM's next task is to communicate the policy to employees. If the individuals for whom the system is intended remain ignorant of its existence or unsure how it works, the PM's efforts are in vain. The information element in the organizational model is a combination of preventive and detective controls. Employees need preventive notification and training, and, should they become aware of an offense, information on how to notify management through established detective controls.

The PM should begin by ensuring that all managers and supervisors, from the top and working down, are fully trained in and committed to the whistleblowing policy. As previously referenced, an organization needs robust buy-in from upper management. Once management is comfortable with the new policy, they must introduce it to their employees in a simple, easy-to-digest manner. Training should be conducted by manager in person, not pushed out as a mandatory online-training module. The training should explain what the PM considers fraud and emphasize zero tolerance for wrongdoing, whether internal or external.

At minimum, employees should walk away knowing where they can seek further information and obtain help in reporting possible offenses. They should know they may speak freely without fear of reprisal and that there are procedures to report either internally or externally.

The PM should hang posters communicating zero tolerance and hotline information. Any changes to the policy should be distributed in a concise and timely manner, and fraud statistics, including updates, number of tips, and actions taken, should be readily available to demonstrate that management is taking real action. While the PM's efforts towards communication are the most voluminous and open, the tips and information the employees may return to the PM are the main objective of this communicative element.

5. Rewards

Tips are consistently and by far the most common fraud-detection method used by employees (Ratley, 2014), accounting for more than 42 percent of frauds detected (see Figure 5). The PM must set up easy-to-use hotlines and encourage employees to use them. Not everyone is a golden citizen willing to go out of his way to blow the whistle. For this reason, PMs should offer rewards for whistleblowers, within the program's means. A government organization is somewhat limited in its ability to offer monetary rewards, but paid leave, VIP parking, and flexible work schedules may be considered.

The PM's internal team and third-party whistleblower representative must stay up to date on federal and state incentives so as to leverage new and existing statutes to their advantage. The PM should provide guidance on how to tap into these programs, which generally offer much larger cash rewards—up to 30 percent of recovered damages from the FCA, 15 to 30 percent from the IRS, and the 10 to 30 percent of total monetary value reclaimed from the SEC.

An extrinsic reward such as cash may not be needed to convince certain employees; those with a strong sense of moral duty are likely to report fraud without expectation of gain. To achieve the greatest probability of reportage, PMs should

combine an external motivator such as cash with a healthy work environment that honors duty and responsibility.

While some fraud is inevitably found wherever human beings conduct transactions, much can be done to reduce occurrences and encourage healthy whistleblowing through simple but emphatic and widely understood policies. The U.S government has a fiduciary duty to its stakeholders, the American people, to pursue such policies methodically to reduce fraud and wrongdoing throughout the federal system.

LIST OF REFERENCES

ACFE - Association of Certified Fraud Examiners. (n.d.). *Association of certified fraud examiners*. Retrieved July 27, 2014, from http://www.acfe.com/contact.aspx

Albrecht, S. (2014, July 1). Iconic fraud triangle endures. Retrieved August 1, 2014.

Allen, J.M. & Sawhney, R. (2010). *Administration and management in criminal justice, a service quality approach.* Chap 2. Open Versus Closed Systems, SAGE Publications, Inc.

Avakain, S. & Roberts, J. (2011). Whistleblowers in organizations: prophets at work? *Journal of Business Ethics* (2012) 110:71–84

Bateman, T. S. & Crant, J. M. (2003). Revisiting intrinsic and extrinsic motivation. Medonza College of Business, University of Notre Dame.

Brainin, S., Kernodle, J., McKenna, S., Morrison, B., Woodruff, K., Cardenas, A., et al. Year in review False Claims Act . *2013 Haynes and Boone Year in Review*, 4.

Breckenridge Institute Center for Management Consulting (2013). *Our Organizational Model.* Retrieved July 10, 2013, from http://www.breckenridgeinstitute.com/our-model.htm

Brooks, L. J. & Dunn, P. (2010). Business & professional ethics for directors, executives & accountants, p. 256, 5th edition, Cengage Learning

Bumgardner, L.. (2003). Reforming corporate America: How does the Sarbanes-Oxley Act impact American business? *Graziadio Business Review,* 6 (1).

Carson, T., Vedru, M. E.,, & Wokutch, R. (2007). Whistle-blowing for profit: An Ethical Analysis of the Federal False Claims Act. *Journal of Business Ethics* (2008) 77:361–376

Claims act cases in fiscal year 2013. Retrieved July 27, 2014, from http://www.justice.gov/opa/pr/2013/December/13-civ-1352.html

Coady, M., & Bloch, S. (1996). *Codes of ethics and the professions.* Melbourne: University Press Melbourne.

Cressey, D. (1973). *Other people's money: Study in the social psychology of embezzlement*. Montclair, NJ: Wadsworth Publishing Company . (Original work published 1953)

Defense Procurement Fraud Law Enforcement: Hearing Before the Subcommittee on Administrative Practice and Procedure of the Committee on the Judiciary United States Senate. 99th Cong. 10 (1985).

Devine, S., & Devine, T. "Whistleblower witch hunts: The smokescreen syndrome." Government Accountability Project (November 2010).

Devine, T & Maassarani, T. F. 2011. *The corporate whistleblower's survival guide.* San Francisco: Berrett-Koehler.

Devine, T., Devine S., & Blaylock, D. (2012, Nov 13). GAP commends senate passage of WPEA. Retrieved from http://www.whistleblower.org/press/gap-commends-senate-passage-wpea-0

Dodd–Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. 111–203 (2010)

Draft, R. L. (2001). *Organizational theory and design* (7th ed.). Florence, KY: South-Western College Publishing:

Dutta, R. (2012, December 4). The Dodd-Frank Act and whistleblowers: Broader protection than you might think. [The Whistleblower Blog]. Retrieved from http://blog.thewhistleblowerattorney.com/2012/12/04/the-dodd-frank-act-and-whistleblowers-broader-protection-than-you-might-think/

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review*, *14*(1), 57–74.

Ethics Resource Center. (n.d.). *About ERC*. Retrieved July 27, 2014, from http://www.ethics.org/page/about-erc

False Claims Act Overview. (n.d.). *Taxpayers against fraud education fund*. Retrieved July 27, 2014, from https://www.taf.org/resource/fca/false-claims-act-overview

Feldman, Y., & Lobel, O (2009). The incentives matrix: The comparative effectiveness of rewards, liabilities, duties and protections for reporting illegality (June 7, 2009). *Texas Law Review*, Vol. 87, May 2010; San Diego Legal Studies Paper No. 09–013. Available at SSRN: http://ssrn.com/abstract=1415663 or http://dx.doi.org/10.2139/ssrn.1415663

Ferzinger, M. J., & Currell, D. G. (1999). *Snitching for dollars: The economics and public policy of federal civil bounty programs,1999 U.* Ill. L. REV. 1141, 1167(1999).

Foy, P. (2012, January 1). Contractor to pay $36.9M for defective flares. *Army Times*. Retrieved July 27, 2014, from http://www.armytimes.com/article/20120424/NEWS/204240308/Contractor-pay-36–9M-defective-flares

Fraud Statistics Overview. (2013, January 1). . Retrieved January 1, 2014, from http://searchjustice.usdoj.gov/search?q=cache:2qJh8TEtD4sJ:www.justice.gov/civil/docs_forms/C-FRAUDS_FCA_Statistics.pdf+fraud+statistics+overview&output=xml_no_dtd&ie=iso-8859–1&client=default_frontend&proxystylesheet=default_frontend&site=default_collection&access=p&oe=UTF-8

Gayl, F. Analysis of DOD Report Titled "Marine Corps implementation of the urgent universal needs process for urgent mine resistant ambush protected vehicles" 2 (Jan. 26, 2009) (unpublished information paper, on file with the Government Accountability Project).

Gagnon, S. (2011, January 1). Questions and answers - What's the melting point of steel?. *Questions and Answers - What's the melting point of steel?*. Retrieved July 27, 2014, from http://education.jlab.org/qa/meltingpoint_01.html

Glater, J. (2008, November 1). Lighting up the night, and a legal battle. *The New York Times*. Retrieved July 27, 2014, from http://www.nytimes.com/2008/11/02/business/02flare.html?pagewanted=all&_r=2&

History of the False Claims Act – The Whistleblower Act. (2013). Retrieved July 29, 2013, from http://www.bernlieb.com/whistleblowers/History-Of-The-False-Claims-Act/index.html

Harned, P., Hajiyev, E., Hartz, M., Kelley, J., Lang, K., & Gabriel, R. (2007). An inside view of nonprofit sector ethics. *Ethic's Resource Center's National Nonprofit Ethics Survey*, *4th*, 4.

Headquarters, Department of the Army. (2011). *Army Acquisition Policy* (AR 70-1). Washington DC: U.S. Government Printing Office.

Internal Revenue Service (2010). *2010 Annual Report to Congress*. Retrieved from http://www.taxpayeradvocate.irs.gov/files/ExecSummary_2010ARC.pdf

Internal Revenue Service (2012). *2012 Annual Report to Congress*. Retrieved from http://www.irs.gov/pub/whistleblower/2012%20IRS%20Annual%20Whistleblower%20Report%20to%20Congress_mvw.pdf

Internal Revenue Service (2013). *Internal revenue manual, section 25.2.2, whistleblower awards.* Retrieved from the Internal Revenue Service: http://www.irs.gov/irm/part25/irm_25–002–002.html

Near, J. P., Rehg, M. T., Van Scotter, J. R., & Miceli, M. P. (2004). Does type of wrongdoing affect the whistleblowing process? *Business Ethics Quarterly* (2004) Volume 12, Issue 2, 219–242.

Jones, G. G., & Luscombe, M. A., 12/01/2012, "Tax strategy: IRS whistleblower program ramps up for increased activity," http://www.accountingtoday.com/ato_issues/26_12/IRS-whistleblower-program-ramps-up-for-increased-activity-64735–1.html retrieved 28 Aug 2013.

Kelton, E. (2013, June 26). SEC whistleblower rewards: Larger ones are coming. *Forbes*, Retrieved from http://www.forbes.com/sites/erikakelton/2013/06/26/sec-officials-on-whistleblower-rewards-the-best-is-yet-to-come/

Kohn, S. M. 2011. *The whistleblower's handbook, a step-by-step guide to doing what's right and protecting yourself.* Guilford, CT: Lyons Press.

King, M. E. "Blowing the whistle on the Dodd-Frank amendments: the case against the new amendments to whistleblower protection in section 806 of Sarbanes-Oxley." *American Criminal Law Review* 48 (2011): 1457. Print.

Kurland, N. B. "The defense industry initiative: Ethics, self-regulation, and accountability." *Journal of Business Ethics* 12 (1993): 137–145. Print.

Lemann, N. (2002, November 4). Paper tiger. *The New Yorker*, Retrieved from http://www.newyorker.com/magazine/2002/11/04/paper-tiger?currentPage=all

McShane, S. L. & Von Glinow, M. A. (2012). *Organizational behavior.* New York, NY:McGraw-Hill/Irwin.

Mesmer-Magnus, J. R., and Chockalingam, V. "Whistleblowing in organizations: An examination of correlates of whistleblowing intentions, actions, and retaliation." *Journal of Business Ethics 62* (2005): 277–297. Print.

Millet, B.(1998). Understanding organisations: The dominance of systems theory. *International Journal of Organizational Behaviour*, 1 (1), 1–12

Nam, D., & Lemark, D. J. (2007). The whistle-blowing zone: Applying Barnard's insights to a modern ethical dilemma. *Journal of Management History*, *13*(1), 33–42

Parton, T., Rajarao, V., & Skalak, S. Economic crime in a downturn. *The Global Economic Crime Survey*, 12.

Parton, T., Rajarao, V., Skalak, S., & Anthony, W. Cybercrime: protecting against the growing threat. *Global Economic Crime Survey*, 18.

Pasha, S. (2006, March 16). Enron's whistle blower details sinking ship. *CNN Money*, Retrieved from http://money.cnn.com/2006/03/15/news/newsmakers/enron/index.htm?section=money_topstories

Pierson, J. K., Forcht, K. A. & Bauman, B.M. (1993). Whistleblowing: an ethical dilemma. *Australasian Journal of Information Systems, 1* (1), 58-62.

Ratley, J. Report to the nations on occupational fraud and abuse. *2014 Global Fraud Study*, 8.

Record number of whistleblower cases filed, resolved by OSHA in fiscal 2012. (2013). Retrieved July 20, 2014, from http://www.bna.com/record-number-whistleblower-n17179871993/

Riley, A., Aardema, B., Vosbury, P., Eiff, M., Frautschy, H., Serkenburg, R., et al. (2012). Aircraft materials, processes, & hardware. *Aviation maintenance technician handbook FAA-H-8083–30* (). Newcastle, Wash.: Aviation Supplies & Academics, Inc..

Robertson, S. (2010). Reasons, values, and morality. In J. Skorupski (Ed.) *The Routledge companion to ethics* (pp. 433–443). London: Routledge.

Rocha, E., & Kleiner, B. H. (2005). To blow or not to blow the whistle? That is the question. *Management Research News (2005) 28, 11/12: ABI/INFORM Global pg.80*

Sahni, S. P., & Kumar, V. (2012). Can we blame the climate of an organization for the stress experienced by employees? *Jindal Journal of Business Research*, 1(2) 181–182

Saunders, L. (2014, April 18). IRS pays awards to whistleblowers. *Wall Street Journal.* Retrieved from http://online.wsj.com

Sweet, W. "Dodd–Frank Act Becomes Law." *The Harvard Law School forum on corporate governance and financial regulation* 21 July 2010. Web. 15 August 2013.

Skalak, S. Economic crime: A threat to business globally. *PwC's 2014 Global Economic Crime Survey*, 43.

Treasury Inspector General for Tax Administration (2012). *Improved oversight is needed to effectively process whistleblower claims.* (Reference Number: 2012–30–045). Retrieved from the Treasury Inspector General for Tax Administration: http://www.treasury.gov/tigta/auditreports/2012reports/201230045fr.pdf

U.S. Bureau of Labor Statistics. *Number of jobs held, labor market activity, and earnings growth among the youngest baby boomers: results from a longitudinal survey*. (2012, July 25). Retrieved July 19, 2014, from http://www.bls.gov/news.release/pdf/nlsoy.pdf.

USDOJ: Justice Department recovers $3.8 billion from False Claims Act cases in fiscal year 2013. (n.d.). *USDOJ: Justice Department Recovers $3.8 Billion from False*

U.S. Department of Labor. (2013). *Whistleblower protection program, whistleblower data FY05–12*. Retrieved from http://www.whistleblowers.gov/whistleblower/wb_data_FY05-13.pdf

U.S. Government Accountability Office. (2012). *Whistleblower Protection: Actions needed to improve DOD's military whistleblower reprisal program.* (GAO Publication No. GAO 12–362). Retrieved from U.S. Government Accountability Office: http://www.gao.gov/assets/590/588784.pdf

U.S. Government Accountability Office. (2011). *Tax whistleblowers: Incomplete data hinders IRS's ability to manage claim processing time and enhance external communication.* (GAO Publication No. 11–683). Retrieved from U.S. Government Accountability Office: http://www.gao.gov/new.items/d11683.pdf

U.S. Office of Special Counsel. (n.d.). Disclosure of Wrongdoing website, viewed on 12 July 2014. https://www.osc.gov/Pages/DOW.aspx

U.S. Securities and Exchange Commission. (2012). *Annual report on the Dodd-Frank Whistleblower Program fiscal year 2012.* Retrieved from U.S. Securities and Exchange Commission: http://www.sec.gov/about/offices/owb/annual-report-2012.pdf

U.S. Securities and Exchange Commission, Office of Inspector General, Office of Audits (2013). *Evaluation of the SEC's Whistleblower Program*. (SEC Report No. 511). Retrieved from the U.S. Securities and Exchange Commission Office of Inspector General: http://www.sec.gov/oig/reportspubs/511.pdf

Volz, D. (2013, December 31). Everything we learned from Edward Snowden in 2013. *National Journal*, Retrieved from http://www.nationaljournal.com/defense/everything-we-learned-from-edward-snowden-in-2013–20131231

Watnick, V. "Whistleblower protections under the Sarbanes-Oxley Act." *Fordham Journal of Corporate & Financial Law* 12 (2007): 831–879. Print.

"Whistleblowing: an effective tool in the fight against corruption" Policy position #01/2010 (Berlin 2010) (available online at www.transparency.org)

Whistle-blower. (n.d.). In *Merriam Webster Online,* Retrieved July 12, 2013, from http://www.merriam-webster.com/dictionary/whistle-blower

Whistleblower Protection Act of 1989, 5 U.S.C. § 2302 (1989).

Whistleblower Protection Enhancement Act of 2012, 5 U.S.C. § 2302 (2012).

Whitaker, L. P.. "The Whistleblower Protection Act: An overview" Congressional Research Service Report for Congress (March 12, 2007). http://www.fas.org/sgp/crs/natsec/RL33918.pdf.

Zornick, G. (2013, May 10). The troubling case of Gregory Hicks. *The Nation*, Retrieved from http://www.thenation.com/blog/174290/troubling-case-gregory-hicks

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California